(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年9月4日 (04.09.2003)

PCT

(10) 国際公開番号
WO 03/073689 A1

(51) 国際特許分類[7]: H04L 9/08, 9/14, H04Q 7/38, H04B 7/06

(21) 国際出願番号: PCT/JP03/02174

(22) 国際出願日: 2003年2月27日 (27.02.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-54064 2002年2月28日 (28.02.2002) JP
特願2002-132068 2002年5月7日 (07.05.2002) JP
特願2003-48364 2003年2月25日 (25.02.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 折橋 雅之 (ORIHASHI,Masayuki) [JP/JP]; 〒272-0001 千葉県 市川市 二俣1-12-1-302 Chiba (JP). 村上 豊 (MURAKAMI,Yutaka) [JP/JP]; 〒213-0034 神奈川県 川崎市 高津区上作延532-1-201 Kanagawa (JP). 安倍 克明 (ABE,Katsuaki) [JP/JP]; 〒215-0005 神奈川県 川崎市麻生区 千代ヶ丘8-21-13-F201 Kanagawa (JP). 松岡 昭彦 (MATSUOKA,Akihiko) [JP/JP]; 〒226-0021 神奈川県 横浜市 緑区 北八朔町2108-1-201 Kanagawa (JP).

(74) 代理人: 鷲田 公一 (WASHIDA,Kimihito); 〒206-0034 東京都 多摩市 鶴牧1丁目24-1 新都市センタービル 5階 Tokyo (JP).

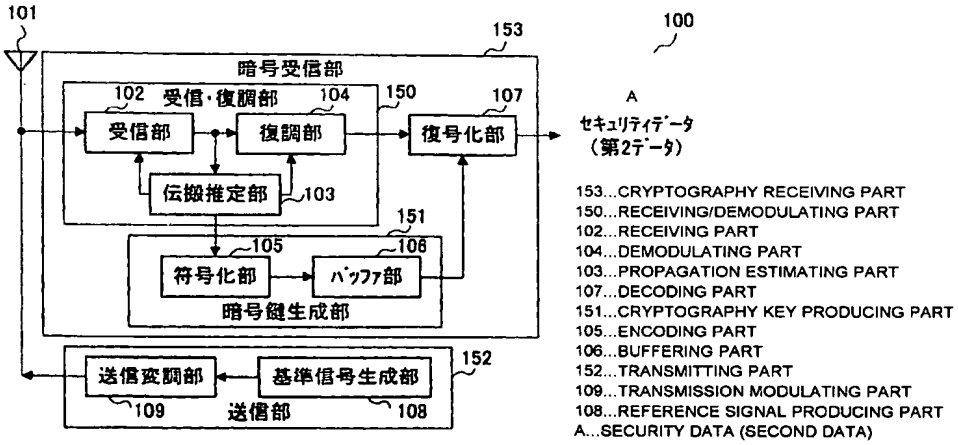
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI

[続葉有]

(54) Title: COMMUNICATION APPARATUS AND COMMUNICATION SYSTEM

(54) 発明の名称: 通信装置及び通信システム



153...CRYPTOGRAPHY RECEIVING PART
150...RECEIVING/DEMODULATING PART
102...RECEIVING PART
104...DEMODULATING PART
103...PROPAGATION ESTIMATING PART
107...DECODING PART
151...CRYPTOGRAPHY KEY PRODUCING PART
105...ENCODING PART
106...BUFFERING PART
152...TRANSMITTING PART
109...TRANSMISSION MODULATING PART
108...REFERENCE SIGNAL PRODUCING PART
A...SECURITY DATA (SECOND DATA)

(57) Abstract: A propagation estimating part (103) uses a reference signal of propagation estimation, sent from the other end of communication, to estimate a propagation environment. This estimation result is sent, as propagation information for reception/demodulation parameters, to a receiving part (102) and a demodulating part (104), thereby removing multipath components from a received signal or performing phase adjustment and the like, in accordance with the propagation information, to output demodulated information.

[続葉有]

WO 03/073689 A1

特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

本発明は、通信相手から送られてきた伝搬推定用の基準信号を用いて伝搬推定部１０３で伝搬環境を推定し、その推定結果を受信復調パラメータ用に伝搬情報として受信部１０２，復調部１０４へと送出され前記伝搬情報に従って受信信号からマルチパス成分を除去、或いは位相の調整などを行いながら復調情報を出力する。

明　細　書

通信装置及び通信システム

技術分野

本発明は、ディジタル通信に用いられる技術であって、特にセキュリティ技術に関する。

背景技術

ディジタル無線通信は、その技術の発展により通信分野の重要な位置を占めるようになってきている。しかしながら、無線通信が公共財である電波空間を利用したものであるため、第３者による受信が可能であるといった根本的な課題を内包している。このため、常に通信内容が第３者により傍受され、情報が漏洩する危険性をはらんでいる。

このような問題を解決するために、通信情報を暗号化するなどして傍受されても情報が漏洩しないような処理を行っているのが現状である。

情報の暗号化は、様々な分野で研究され、また様々な分野で応用されている。これは、通信システムを変更しなくても一定のセキュリティが確保できるといった大きな特長によるところが大きい。

しかしながら、通信情報を暗号化しても第３者による傍受を防ぐことはできないため、第三者により傍受された受信情報から時間をかけることにより暗号化した通信情報が解読されてしまうと言った問題がある。

発明の開示

本発明の目的は、大きな通信システムの変更をすることなしに高いセキュリティを確保することである。

この目的は、通信相手から送信された基準信号を用いて推定した伝搬環境の

情報を秘匿情報として取得することにより達成できる。

図面の簡単な説明

図１は、本発明の実施の形態１に係る通信装置の構成を示すブロック図、

図２は、本発明の実施の形態１に係る通信装置の構成を示すブロック図、

図３は、本発明の実施の形態１に係る通信装置の動作を示すシーケンス図、

図４は、本発明の実施の形態２に係る通信装置における伝搬推定部と符号化部の構成を示すブロック図、

図５は、コードブックを示す図、

図６は、遅延プロファイルを示す図、

図７は、本発明の実施の形態３に係る通信装置の構成を示すブロック図、

図８は、本発明の実施の形態３に係る通信装置の動作を示すシーケンス図、

図９は、本発明の実施の形態４に係る通信装置の構成を示すブロック図、

図１０は、本発明の実施の形態４に係る通信装置の構成を示すブロック図、

図１１は、本発明の実施の形態５に係る通信装置の動作を示すシーケンス図、

図１２は、本発明の実施の形態６に係る信号のフレーム構成を示す図、

図１３は、本発明の実施の形態６に係る信号のフレーム構成を示す図、

図１４は、本発明の実施の形態７に係る通信装置の構成を示すブロック図、

図１５は、本発明の実施の形態７に係る通信装置の構成を示すブロック図、

図１６は、本発明の実施の形態８に係る通信装置における伝搬推定部の構成を示すブロック図、

図１７は、到来方向推定結果を説明する図、

図１８は、本発明の実施の形態９に係る通信装置の構成を示すブロック図、

図１９は、偏波状態を説明する図、

図２０は、本発明の実施の形態１０に係る通信装置の構成を示すブロック図、

図２１は、本発明の実施の形態１１に係る通信装置の構成を示すブロック図、

図２２は、本発明の実施の形態１２に係る通信装置の構成を示すブロック図、

図２３は、本発明の実施の形態１３に係る通信装置の構成を示すブロック図、

図２４は、本発明の実施の形態１３に係る通信装置の構成を示すブロック図、

図２５は、本発明の実施の形態１３に係る通信装置の動作を示すシーケンス図、

図２６は、本発明の実施の形態１４に係る通信装置の構成を示すブロック図、

図２７は、本発明の実施の形態１４に係る通信装置における伝搬推定部の構成を示すブロック図、

図２８は、自己相関系列を示す図、

図２９は、遅延プロファイルを示す図、

図３０は、本発明の実施の形態１５に係る通信装置における伝搬推定部の構成を示すブロック図、

図３１は、本発明の実施の形態１６に係る通信装置の構成を示すブロック図、

図３２は、本発明の実施の形態１６に係る通信装置における伝搬推定部、変換部及び符号化部の構成を示すブロック図、

図３３は、本発明の実施の形態１６に係るシステムブロック図、

図３４は、遅延プロファイルの周波数特性を示す図、

図３５は、本発明の実施の形態１７に係る通信装置の構成を示すブロック図、

図３６は、本発明の実施の形態１７に係る通信装置の構成を示すブロック図、

図３７は、本発明の実施の形態１７に係る通信装置の動作を示すシーケンス図、

図３８は、本発明の実施の形態１７に係る通信装置の信号処理を示す図、

図３９は、本発明の実施の形態１７に係る通信装置の信号処理を示す図、

図４０は、電力分布を示す図、

図４１は、電力分布を示す図、

図４２は、電力分布を示す図、

図４３は、本発明の実施の形態１８に係る通信装置の構成を示すブロック図、

図４４は、本発明の実施の形態１８に係る通信装置の構成を示すブロック図、

図４５は、本発明の実施の形態１８に係る通信装置の信号処理を示す図、

図４６は、本発明の実施の形態１９に係る通信装置の構成を示すブロック図、

図４７は、本発明の実施の形態１９に係る通信装置の動作を示すシーケンス図、

図４８は、本発明の実施の形態２０に係る信号のフレーム構成を示す図、

図４９は、本発明の実施の形態２０に係る信号のフレーム構成を示す図、

図５０は、本発明の実施の形態２１係る信号のフレーム構成を示す図、

図５１は、本発明の実施の形態２２に係る通信装置の構成を示すブロック図、

図５２は、本発明の実施の形態２２に係る信号のフレーム構成を示す図、

図５３は、本発明の実施の形態２３に係る通信装置の構成を示すブロック図、

図５４は、本発明の実施の形態２３に係る信号のフレーム構成を示す図、

図５５は、本発明の実施の形態２４に係る通信装置の構成を示すブロック図、

図５６は、本発明の実施の形態２４に係る通信装置の構成を示すブロック図、

図５７は、本発明の実施の形態２５に係る通信装置の構成を示すブロック図、

図５８は、本発明の実施の形態２５に係る通信装置の構成を示すブロック図、

図５９は、本発明の実施の形態２７に係る通信装置を用いた通信システムを示す図、

図６０は、本発明の実施の形態２７に係る通信装置の構成を示すブロック図、

図６１は、本発明の実施の形態２７に係る通信装置の動作を示すシーケンス図、

図６２は、本発明の実施の形態２７に係る通信装置の動作を示すシーケンス図、

図６３は、本発明の実施の形態２７に係る通信装置の動作を示すシーケンス図、

図６４は、信号の送信状態を時間軸で示した図、

図６５は、信号の送信状態を時間軸で示した図、

図６６は、信号の送信状態を時間軸で示した図、

図６７は、信号の送信状態を時間軸で示した図、

図６８は、本発明の実施の形態２６に係る通信装置を用いた通信システムを示す図、

図６９は、本発明の実施の形態２６に係る通信装置を用いた通信システムを示す図、

図７０は、本発明の実施の形態２６に係る通信装置を用いた通信システムを示す図、

図７１は、電力分布を示す図、

図７２は、伝搬パラメータの直交性の時間的変化を示す図、

図７３は、通信品質をビットエラーレート（ＢＥＲ）で表した図、

図７４は、通信品質をビットエラーレート（ＢＥＲ）で表した図、

図７５は、信号の送信状態を時間軸で示し図、

図７６は、電力分布を示す図、

図７７は、本発明の実施の形態２８に係る通信装置を用いた通信システムを示す図、及び

図７８は、本発明の実施の形態２８に係る通信装置の受信処理を示した図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を用いて説明する。

（実施の形態１）

伝搬情報をセキュリティの暗号鍵情報として利用する発明について図１、図２および図３を用いて説明する。図１は本実施の形態１に係る通信装置である暗号受信装置の具体的構成を示し、図２は暗号送受信装置の具体的構成を示したものである。図３は端末間の通信手続きを記述したものである。ここでは便宜上、図３中の基地局を図２に示した暗号送受信装置、端末を図１で示した暗号受信装置であるものとして説明を行うが、その組合せを制限するものではな

く、両者が図２で示す暗号送受信装置であっても構わない。

図１はアンテナ１０１と、暗号受信部１５３と、送信部１５２とで構成されている。暗号受信部１５３は受信したＲＦ信号から伝搬状態を推定し、これを暗号鍵として暗号の復号を行いセキュリティデータを出力するものであり、受信復調部１５０と、暗号鍵生成部１５１と、復号化部１０７とで構成されている。送信部１５２は基準ＲＦ信号を出力するものであり、基準信号生成部１０８、送信変調部１０９とからなる。アンテナ１０１は電波を受信・送信しＲＦ信号を入出力するものであり、受信復調部１５０はＲＦ信号を入力し、伝搬情報と復調情報とを出力するものであり、受信部１０２、伝搬推定部１０３、復調部１０４とからなる。

受信部１０２はＲＦ信号と伝搬情報を入力し、ＲＦ信号を適切な受信状態に制御し、受信信号を出力するものであり、伝搬推定部１０３は受信信号から伝搬特性を推定し伝搬情報を出力するものであり、復調部１０４は受信信号と伝搬情報とから適切な復調を行い復調情報を出力するものである。暗号鍵生成部１５１は伝搬情報を入力し暗号鍵情報を出力するものであり、符号化部１０５とバッファ部１０６とで構成されている。

符号化部１０５は伝搬情報から特徴を抽出し暗号鍵（第１データ）を生成・出力するものであり、バッファ部１０６は符号化された暗号鍵を記憶し、記憶した暗号鍵情報を出力するものである。復号化部１０７は暗号鍵情報と復調情報とを入力し、暗号鍵情報から復調情報の暗号を復号化しセキュリティデータ（第２データ）を出力するものである。基準信号生成部１０８は予め定められた基準信号を生成し出力するものであり、送信変調部１０９は基準信号を入力しＲＦ信号に変調・出力するものである。

図２はアンテナ２０１と、暗号受信部２５３と、暗号送信部２５４とで構成されている。アンテナ２０１および暗号受信部２５３は、図１中での対応する部位と同等の機能を有している。暗号送信部２５４はセキュリティデータと暗号鍵情報とを入力し、伝搬推定用の基準信号と、暗号鍵情報とセキュリティデ

ータとから予め定められた方法により暗号化される暗号化情報と、を切り換えて変調・出力するものであり、送信変調部２５２と、基準信号生成部２０８と、暗号化部２０９と、切換部２１０とで構成される。

送信変調部２５２は選択された通信情報を変調しＲＦ信号を出力するものであり、変調部２１１と送信部２１２とから構成されている。基準信号生成部２０８は予め定められた基準信号を生成し出力するものであり、暗号化部２０９は暗号鍵情報とセキュリティデータとを入力し、暗号鍵情報からセキュリティデータを暗号化し、暗号情報を生成・出力するものである。切換部２１０は基準信号と暗号情報とを入力し、両者のうち１つを選択、通信情報を出力するものであり、変調部２１１は選択された通信情報を変調し変調信号を出力するものであり、送信部２１２は変調信号を送信するＲＦ信号に変換・出力するものである。

以上のように構成された基地局（図２に示される暗号送受信装置）と端末（図１に示される暗号受信装置を含む通信装置）とは、図３のような手順で通信を行っている。

以下、図１に示された装置の動作を説明する。アンテナ１０１は、電波を受信しＲＦ信号を出力する。受信されたＲＦ信号は、受信復調部１５０に入力され伝搬情報と復調情報とが出力される。まず、受信部１０２はＲＦ信号と伝搬情報を入力し、伝搬情報に従い、ゲインを一定に保ったり、周波数・時間ずれを修正したりすることで受信状態を最適に保つように制御しながら受信信号を出力する。伝搬推定部１０３は受信信号を入力し、受信時刻、伝搬時間、周波数状態、偏波状態、受信電力、マルチパス状態、位相状態、伝搬歪などを検出する。

それぞれの状態は、受信復調パラメータ用に伝搬情報として受信部１０２、復調部１０４へと送出されると同時に、暗号鍵生成部１５１へも送出される。復調部１０４は、受信信号と伝搬情報とを入力し、伝搬情報に従って受信信号からマルチパス成分を除去、或いは位相の調整などを行いながら復調し、復調

情報を出力する。暗号鍵生成部１５１は受信復調部１５０から出力された伝搬情報から伝搬状態の特徴を抽出し、暗号鍵を生成・記憶し、暗号鍵情報を出力する。

符号化部１０５は伝搬推定部１０３から出力された伝搬情報を入力し、その中から受信信号の伝搬状態の特徴を抽出する。例えば、マルチパス状態を例に挙げると、複数の伝搬路により形成されるマルチパス伝搬において、そのマルチパス特性は相関関数などを用いて検出することが可能である。

このようにして求められたマルチパスの電界情報のうち、最大のパワーを検出したパス成分の遅延時間とパワーとから予め定められた方法に従って符号化を行い、暗号化に用いる暗号鍵を生成・出力する。生成された暗号鍵は、バッファ部１０６で入力され記憶されて、暗号鍵情報が出力される。復号化部１０７は、復調情報と暗号鍵情報を入力し予め定められた方法に従って復調情報を復号し、セキュリティデータを出力する。送信部１５２は基準信号を生成した後、変調しＲＦ信号を出力する。基準信号生成部１０８は、通信対象の相手端末に対して伝搬状態を推定するための基準信号を生成し、これを出力する。送信変調部１０９は基準信号を入力し、変調・周波数変換などによりＲＦ信号を出力する。出力されたＲＦ信号は、アンテナ１０１から放射される。

次に、図２に示された装置の動作を説明する。ここでは、図１に示した装置からの相違点のみを示す。

アンテナ２０１から入力されたＲＦ信号が、復号化部２０７を通じて復号されセキュリティデータが出力されるまでの暗号受信部２５３は、図１の対応する部位と同一の構成である。暗号送信部２５４は、暗号鍵情報とセキュリティデータを入力し、送信するＲＦ信号を出力する。基準信号生成部２０８は、通信対象の相手端末に対して伝搬状態を推定するための基準信号を生成し、出力する。暗号化部２０９は、暗号鍵情報とセキュリティデータとを入力し、予め定められた方法に従って暗号化した暗号化情報を出力する。

切換部２１０は、基準信号生成部２０８から入力される基準信号と、暗号化

部２０９から入力される暗号化情報の一方を選択し選択された通信情報を出力する。選択された通信情報は、送信変調部２５２により変調され送信信号に変換されてＲＦ信号を出力する。即ち、通信情報は、変調部２１１に入力され所定の変調が施されて変調部２１１より変調信号として出力される。次に、変調信号は、送信部２１２へ入力され、ＲＦ信号に変換されて送信部２１２より出力される。このＲＦ信号はアンテナ２０１を介して放射される。

以上の動作を、通信手順の観点から図３を用いて説明する。

（０）基地局、端末：初期化

基地局、端末共に、電源が投入された直後、或いは特定の信号を受けて初期状態にセットされる。同時に、周波数や時間同期などの状態は事前に定められた手順に従ってセットされる。

以上のこれらの初期動作が終了した一定時間後、基地局は一定時間毎に制御情報を制御信号に載せて送信する。

一方、端末は初期動作が終了した後、制御信号のサーチを始める。端末が基地局から送信した制御信号を受信すると、その時刻、周波数などを検出してシステムが保有する時刻・周波数に同期する（システム同期）。システム同期が正常に終了した後、端末はその存在を基地局に通知するために登録要求信号を送信する。基地局は、端末からの登録要求に対して、登録許可信号を送信することで端末の登録許可を行う。

（１）基地局：第１基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第１基準信号として出力する。具体的には、切換部２１０は基準信号生成部２０８で生成される基準信号を選択し、送信変調部２５２へ出力する。送信変調部２５２は選択された通信情報をＲＦ信号としてアンテナ２０１から放射する。

端末では、基地局からの信号を待っており、伝搬推定部１０３は受信した受信信号から第１基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。符号化部１０５は、伝搬推定部１０３からの伝搬情報を入力

し、伝搬状態の特徴抽出をおこなう。次に抽出した特徴情報を用いて暗号鍵への変換を行う。この部分の動作は別途詳細に説明する。この符号化部１０５が抽出する特徴や、それを暗号鍵へ変換する方法については基地局と端末の間で予め共有しておくものとする。変換された暗号鍵はバッファ部１０６に保持され暗号鍵情報が出力される。この暗号鍵を第１鍵として基地局は以降の通信の暗号鍵とする。

（２）端末：第２基準信号送信

端末は、（１）と同様に基地局で行う伝搬推定用の基準信号を第２基準信号として出力する。

基地局では、端末からの信号を受信すると第２基準信号を検出し、伝搬推定部２０３は受信信号と既知信号である基準信号とから伝搬推定を行う。（１）と同様、伝搬推定部２０３が出力する伝搬情報は、符号化部２０５によって暗号鍵へと変換され、バッファ部２０６で暗号鍵情報が保持、出力される。この暗号鍵を第２鍵として端末は以降の通信の暗号鍵とする。

（３）基地局：暗号送信

基地局は、切換部２１０の状態を、暗号化部２０９から出力される暗号化情報を選択するように切り換える。暗号化部２０９は（２）で得られた第２鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化情報を出力する。暗号化情報は切換部２１０で選択され、通信情報が送信変調部２５２へと出力される。送信変調部２５２は通信情報を変調し、ＲＦ信号としてアンテナ２０１から暗号化信号を放射する。

端末は、暗号化信号を受信すると受信復調部１５０が受信信号を復調情報へと復調する。復号化部１０７は復調情報と（１）で求めた第１鍵を用い、予め定められた方法によって暗号の復号化を行いセキュリティデータを出力する。以下、（３）の暗号通信や通常の通信を繰り返す。

さて、通信端末間で形成される伝搬路はその相対的な位置や空間形状、反射物などにより一意に決まり、それは基地局から端末に対して形成される伝搬状

態と、端末から基地局に対して形成される伝搬状態は光伝搬の相反性により同一であることが知られている。このことは、（１）で求められる伝搬状態と（２）で求められる伝搬状態（例えば、遅延プロファイルなど）は同一の結果が求まることとなることがわかる。また、基地局と端末の間では、予め伝搬情報から暗号鍵へ変換する手順を共有してある。則ち、（１）で得られる暗号鍵（第１鍵）と（２）で得られた暗号鍵（第２鍵）は同一となり、通信端末間においては共有鍵として用いることが可能な状態となっている。この結果、（３）の通信手順においては共有鍵で暗号化・復号化を行うこととなり、基地局で暗号化された情報は端末で正常に復号化されることになる。

この状況で全通信を第３者が第３の端末を用いて傍受した場合を考える。先に説明したとおり、伝搬路は基地局と端末との間で形成される伝搬空間で求まるものである。このため、基地局や端末から物理的に異なった位置で（１）から（３）までの通信を観察している場合、第３の端末と基地局或いは端末間で形成される伝搬特性は、（１）や（２）で求められるそれとは異なってくる。その上、基地局と端末間では暗号化の為の鍵の授受を行っているわけではないため、第３の端末がこれを知ることは出来ない。

このことから、通信の物理層において高いセキュリティを確保できることが分かる。また、これらの処理は基本的に従来の算術的な手法を用いた暗号化、復号化とは独立して行うことが可能であるため、従来技術に加えて本発明を実施することでより高いセキュリティが期待できるといった有利な特長を有する。

この説明において、初期化作業である（０）について説明を行ったが、これは一般的な運用を想定したものであり、本発明に必要な手続きではない。

また、（１）や（２）で基準信号を送信することで、互いの伝搬状態を推定するとしたが、これは一般に既知信号としての基準信号を用いた方が精度を高く推定できるためであって、伝搬推定では特に基準信号を用いなくても可能なことはいうまでもない。換言すれば、例えば（０）で行っている制御信号、登

録要求信号や登録許可信号などを利用して伝搬推定を行うことも可能である。

以上の発明は、伝搬状態を暗号鍵として利用することを特徴としているため、基地局や端末の移動が発生すると、問題が生ずる虞がある。この場合、図３に示した（１’）、（２’）、（３’）のように繰り返し基準信号の送受信を行うことで、この問題を回避することも可能である。

このように、本実施の形態１の通信装置及び通信システムによれば、伝搬推定部１０３が基準信号に基づいて伝搬環境を推定して相関関数等の伝搬パラメータである推定値を出力するとともに、符号化部１０５は推定値より得られたデータを出力するので、基地局と端末間で暗号化の為の鍵の授受を行う必要がないために第３の端末がこれを知ることは出来ず、通信の物理層において大きな通信システムの変更をすることなしに高いセキュリティを確保することができる。また、本実施の形態１の通信装置及び通信システムによれば、従来の算術的な手法を用いた暗号化、復号化とは独立した処理によりセキュリティを確保することができるので、従来の暗号化、復号化技術と併用することにより極めて高いセキュリティを確保することができる。また、本実施の形態１の通信装置及び通信システムによれば、伝搬状態に応じて符号化パターンを変化させることができるので、環境変化に強い通信を行うことができる。また、本実施の形態１の通信装置及び通信システムによれば、推定した伝搬環境より伝搬パラメータを求めて暗号鍵を取得することができるので、無変調の信号によって情報を送受信することができる。

なお、本実施の形態１においては、バッファ部１０６から出力される暗号鍵情報を復号化部１０７にてセキュリティデータを復号化する際の暗号鍵として用いることとしたが、これに限らず、バッファ部１０６から出力される暗号鍵情報を復号化部１０７にて復号化されるセキュリティデータ以外の他のセキュリティデータを復号化する際の暗号鍵として用いても良い。この場合には、復号化部１０７は不要になる。また、本実施の形態１においては、伝搬状態を示すパラメータとして遅延プロファイルを用いたが、偏波面や旋回方向などの

偏波状態を用いたり、位相情報を用いたり、伝搬遅延時間を用いたり、到来方向推定情報を用いたり、受信電力情報を用いたり、或いは、様々なパラメータの組み合わせを用いたりすることも考えられる。こうすることで、第３の端末の観測がより複雑化するため高度なセキュリティを確保できる。特に、偏波や位相を用いることで、それらが伝搬環境に大きく左右されることから、他の端末からの推定を一層困難にするといった特徴を有する。

さらに、複数のアンテナ２０１に複数のアンテナエレメントで構成するアレイアンテナ構造を適用することで、伝搬推定のパラメータとして到来方向の要素を付加することができる。こうすることでより柔軟なシステムを構成が可能となる。

また、上記においては、変調方式、多重化方式について説明していないが、本方式は原理的にどの変調方式にも適用できることは明白であり、現在行われているＰＳＫ変調、ＱＡＭ変調、スターＱＡＭ変調、或いはＴＤＭＡ、ＦＤＭＡ、ＳＳ（ＦＨやＣＤＭＡ）、ＯＦＤＭ、あるいは空間多重（ＳＤＭやＭＩＭＯ）などあらゆるものに適用可能である。

さらに、通信手順で、基準信号を送信する際、第１基準信号の送信と第２基準信号の送信を行っているが、両者はどちらが先に実施されても本方式に影響を与えるものではないことは明白である。また、通信手順の中で基準信号を別途通信しているが、これは、後述する図１２のフレーム構成（ｂ）、（ｃ）のように、データストリームの中に基準信号を挿入することで、（１）と（３）の手順を同時に実施することができるといった有利な特長を有することが出来る。

（実施の形態２）

本実施の形態２に係る通信装置は、伝搬推定と暗号鍵への変換方法について説明するものであり、図１に示す本発明の実施の形態１に係る通信装置１００において、伝搬推定部１０３と符号化部１０５を図４に示す構成とするものである。なお、伝搬推定部１０３と符号化部１０５以外の構成は、図１と同一構

成であるのでその説明は省略する。

ここでは伝搬状態を示すパラメータとして代表的な遅延プロファイルを扱うものとして説明する。この遅延プロファイルは、各パス成分の遅延時間と、パワー、位相などが含まれている。ここでは、パス成分の遅延時間とパワーとを扱った例を示す。

図１中の伝搬推定部１０３は基準信号が含まれる受信信号を取り出し、伝搬状態の推定を行う。伝搬状態として遅延プロファイルを求める場合、遅延プロファイルは基となる信号と受信した信号との相関で求められることが知られている。この場合、伝搬推定部１０３は既知信号である基準信号を用いて、その信号系列と受信信号系列の相関値を算出することで遅延プロファイルが得られる。

このようにして得られた伝搬情報は符号化部１０５によってその特徴が抽出される。特徴抽出の例としてベクトル量子化手法を用いるものが考えられる。これは、代表的な遅延プロファイルのテンプレートを量子化ベクトルとして参照テーブル上に幾つか用意しておき、更に各量子化ベクトルに対応させた暗号鍵を参照テーブル上に格納しておく。符号化部１０５は、このように用意しておいた参照テーブルから伝搬推定部１０３が推定した結果と照合し、最も類似性の高い遅延プロファイルのテンプレートに対応する暗号鍵を選択・出力する。

以上、伝搬状態を推定し、暗号鍵へと符号化する方法について説明したが、図４を用いてさらに詳細に説明する。

図４は、伝搬推定部１０３と符号化部１０５を示している。これらは図１の各部位に相当する機能を更に詳細に示したものである。図１の説明では、伝搬推定部１０３は周波数・時間ずれや位相情報など様々な状態を推定するものとしたが、ここでは遅延プロファイルを推定する方法についてのみ説明する。

伝搬推定部１０３は、バッファ４０１と、基準信号系列格納部４０２と、コンボルバ４０３と、バッファ４０４とからなり、符号化部１０５は、量子化部４０５と、変換部４０６、コードブック４０７とからなる。バッファ４０１は、

入力した受信信号を一定長だけ一時保持するものであり、基準信号系列格納部４０２は予め定められた基準信号系列を格納、順次出力するものであり、コンボルバ４０３は一時保持された受信信号と基準信号系列を畳み込み演算して相関値を出力するものであり、バッファ４０４は算出された相関系列を一時保持するものである。量子化部４０５はコードブック４０７に記録された量子化ベクトルの中から、入力されたベクトル列に最も類似したものを検索しコードを出力する。変換部４０６は、量子化部４０５が出力するコードに対応する暗号鍵（第１データ）をコードブックから選択し、出力する。

コードブック４０７は、この中には量子化ベクトルと暗号鍵が格納されている。図５は遅延プロファイルのテンプレートとなる量子化ベクトルと、それに対応する暗号鍵とが格納されたコードブックの例を示している。

次に、伝搬推定部１０３と符号化部１０５の動作を説明する。

まず、伝搬推定部１０３は、基準信号を含む受信信号をバッファ４０１に保持する。コンボルバ４０３は、基準信号系列格納部４０２からの基準信号系列と、バッファ４０１に保持された受信信号系列とのスライディング相関を演算した結果を相関系列として出力し、それらを順次バッファ４０４に保持する。バッファ４０４で保持された相関系列は、基準信号系列と受信信号系列との相関値、則ち遅延プロファイルに相当するデータが格納されている。これらの遅延プロファイル情報は、一連の入力ベクトルとして符号化部１０５へと送出される。この様にして求められる遅延プロファイル情報の一例を図６に示す。

量子化部４０５は、バッファ４０４からの入力ベクトルと、コードブック４０７の量子化ベクトルに記録されたベクトルとを照合し、類似性の最も高いものを抽出し、その対応コードを出力する。具体的には、入力ベクトルをＸｉｎ、コードｍの量子化ベクトルをＸｑｍ（ｍ：１～Ｍ）とすると、

$$d = |Xin - Xqm|^2 \qquad (1)$$

が最小になるＸｑｍを求めることとなる。このようにして求めた量子化ベクト

ルの対応コードｍを出力する。

変換部４０６は遅延プロファイルの対応コードｍと、コードブックの暗号鍵テーブルの内容とから対応する暗号鍵を出力する。このような構成で暗号鍵を決定することにより、柔軟な暗号鍵の設定が簡単な回路で実現可能になる。

このように、本実施の形態２の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、伝搬推定部１０３は遅延プロファイルを生成して推定値として基準信号との相関関数を求めるとともに、符号化部１０５は相関関数と暗号鍵が対応付けられたコードブックを用いて伝搬推定部１０３から入力した推定値に対応した暗号鍵情報を読み出すので、柔軟な暗号鍵の設定が簡単な回路で実現可能になる。また、本実施の形態２の通信装置及び通信システムによれば、伝搬パラメータをベクトル量子化して遅延プロファイルを求めるので、安定した伝搬パラメータの設定を行うことができる。

なお、本実施の形態２においては、符号化部１０５の遅延プロファイルの符号化方法として量子化ベクトル手法を用いる方法について説明したが、遅延プロファイルのデータ系列を評価式で近似し、それから得られる近似式の係数を利用するなどして符号化する事や、遅延プロファイルを幾つかのブロックに分割して、その大きさや、順番から符号化したり、最大パワーを有するパスの遅延時間とその大きさによって符号化したりするなど様々な方法が考えられる。

（実施の形態３）

本発明の実施の形態３に係る通信装置７００は、図２に示す本発明の実施の形態１に係る通信装置２００において、伝搬制御部７０１を追加し、かつ符号化部２０５の代わりに符号化部７０３を有し、変調部２１１の代わりに変調部７０４を有し、送信部２１２の代わりに送信部７０５を有している。なお、図２と同一構成である部分は同一の符号を付してその説明は省略する。

以下に、伝搬制御により安定した通信方法の発明について、図７および図８を用いて説明する。

図７の送受信装置７００は、複数のアンテナ素子から構成されるアンテナ２

０１、暗号受信部７０６、暗号送信部７０７を具備する。暗号受信部７０６は受信復調部７０８と、暗号鍵生成部２５１と、復号化部２０７とで構成されており、図１の各部位と同じ構成でなっている。暗号送信部７０７は、基準信号生成部２０８と、暗号化部２０９と、切換部２１０と、送信変調部７０９とからなっており、基準信号生成部２０８、暗号化部２０９、切換部２１０は図２中の対応する部位と同じである。

送信変調部７０９は、伝搬制御部７０１と、変調部７０４と、送信部７０５とで構成されている。伝搬制御部７０１は伝搬推定部２０３から出力される伝搬情報と、符号化部７０３が伝搬情報から特徴を抽出した伝搬特徴情報（第１データ）とを入力し、通信相手の端末に対しての伝搬状態が最適になるように制御するよう、変調制御信号と、送信制御信号とを出力するものである。変調部７０４は伝搬制御部７０１から出力された変調制御信号と通信情報とを入力し、変調制御信号に基づき位相や出力タイミング、振幅の微調整などを行いながら通信情報を変調し、各アンテナ素子に対応する変調信号を出力するものである。

送信部７０５は、送信制御信号と変調信号とを入力し、送信制御信号に基づき、周波数や出力タイミングなどを制御しながら変調信号を、各アンテナ素子に対応するＲＦ信号へ変換しアンテナ２０１へと出力するものである。

以上のように構成された通信装置について、図８の通信手続きを用いながらさらに詳細に説明する。図８において、基地局、端末ともに図７に示す通信装置として説明を行う。なお、ここでは第１の実施の形態からの相違点のみを記述する。

（０）基地局、端末：初期化

第１の実施の形態と同様な動作を行う。

（１）基地局：第１基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第１基準信号として出力する。具体的には、切換部２１０は基準信号生成部２０８で生成される基準信号を選

択し、送信変調部７０９へ出力する。送信変調部７０９では選択された通信情報と、伝搬情報と伝搬特徴情報とを入力し、通信相手である端末への伝搬状態を制御しながらＲＦ信号を出力しアンテナ２０１から放射する。この伝搬制御については別途詳細に説明する。

端末は基地局からの信号を待っており、伝搬推定部２０３は受信した受信信号から第１基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。この推定値である伝搬情報は、符号化部７０３と伝搬制御部７０１へ送出される。符号化部７０３は、伝搬推定部２０３からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴情報を伝搬制御部７０１へ出力する。同時に、抽出した伝搬特徴情報を用いて暗号鍵への変換を行う。変換された暗号鍵はバッファ部２０６に保持され暗号鍵情報が出力される。この暗号鍵を第１鍵として基地局は以降の通信の暗号鍵とする。

（２）端末：第２基準信号送信

端末は、（１）と同様に基地局で行う伝搬推定用の基準信号を第２基準信号として出力する。この時、伝搬制御部７０１は（１）で求めた伝搬情報と、伝搬特徴情報とから、通信相手である基地局に対して暗号鍵（第１鍵）に対応する伝搬状態になるように変調部７０４と送信部７０５を制御しながら第２基準信号を送信する。

基地局では、端末からの信号を受信すると第２基準信号を検出し、伝搬推定部２０３は受信信号と既知信号である基準信号とから伝搬推定を行う。（１）と同様、伝搬推定部２０３は伝搬情報を出力し、符号化部７０３は伝搬情報から伝搬特徴情報を抽出して出力する。さらに伝搬特徴情報から暗号鍵へと変換され、バッファ部２０６で暗号鍵情報が保持される。この暗号鍵を第２鍵として端末は以降の通信の暗号鍵とする。

（３）基地局：暗号送信

基地局は、切換部２１０の状態を、暗号化部２０９から出力される暗号化情報を選択するように切り換える。暗号化部２０９は（２）で得られた第２鍵を

用いてセキュリティデータを予め定められた方法で暗号化し、暗号化情報を出力する。暗号化情報は切換部２１０で選択され、選択された通信情報が送信変調部７０９へと出力される。送信変調部７０９では、伝搬制御部７０１が（２）で求めた伝搬情報と、伝搬特徴情報とから、通信相手である端末に対して暗号鍵（第２鍵）に対応する伝搬状態になるように変調部７０４と送信部７０５を制御しながらＲＦ信号としてアンテナ２０１から暗号化信号を放射する。

端末は、暗号化信号を受信すると受信復調部７０８が受信信号を復調情報へと復調する。復号化部２０７は復調情報と（１）で求めた第１鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

（４）端末：暗号送信

端末は、（３）と同様に第１鍵を用いて暗号化を行い暗号化情報を出力する。送信変調部７０９では、（１）や（３）で求めた伝搬情報と、（１）で選択した暗号鍵に対応する伝搬特徴情報とから、通信相手である基地局に対して暗号鍵（第１鍵）に対応する伝搬状態になるように変調部７０４と送信部７０５を制御しながらＲＦ信号としてアンテナ２０１から暗号化信号を放射する。基地局は、（３）と同様に（２）で求めた第２鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

第１の実施の形態で示したことと同様、基地局と端末が生成した暗号鍵（第１鍵および第２鍵）は共有鍵として利用が可能である。則ち、（３）や（４）における暗号化・復号化は問題なく処理されることが分かる。

このように、本実施の形態３の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、伝搬制御部７０１は、符号化部７０３にて生成した暗号鍵と同一の暗号鍵が通信相手においても得られるように変調部７０４と送信部７０５を制御して基準信号を送信する際の伝搬環境を制御するので、通信相手が基準信号を送信する際の伝搬環境と通信相手へ基準信号を送信する際の伝搬環境との誤差を小さくすることができて共通の暗号鍵を生成する際の誤差を小さくすることができる。また、本実施の形態３の通信装置及び通

信システムによれば、送信変調部７０９に於いて受信時で求めた伝搬情報と暗号鍵に対応した伝搬状態を示す伝搬特徴情報とから、通信相手となる端末に対しての伝搬状態を、伝搬特徴情報になるよう制御されているため、受信時の伝搬状態と想定された（暗号鍵に対応する）伝搬状態との誤差が小さくなり、通信品質が大幅に向上するといった有利な特長を有する。

また、伝搬状態が変化した場合でも、伝搬制御を行うことで通信の安定性を向上させることが出来る。

また、暗号鍵を選択する際に符号化部７０３が検索したテンプレートの中で、類似したものが複数存在する場合、送信側が明示的に伝搬状態を制御することで曖昧さを排除する事が出来る。

なお、本実施の形態３においては、通信手順で、基準信号を送信する際、第１基準信号の送信と第２基準信号の送信を行っているが、両者はどちらが先に実施されても本方式に影響を与えるものではないことは明白である。当然、暗号通信の手順も同様で、その順序によって本方式には影響を与えない。

本方式では、基準信号の通信を以て暗号鍵の授受を行っており、基準信号以降の暗号化信号については、その暗号鍵と先に授受したそれとが一致していればよい。つまり、（３）や（４）において送信側が受信側に対して伝搬制御を行いながら通信を行っているが、暗号鍵がしめす伝搬状態と一致する必要はない。

また、通信手順の中で基準信号を別途通信しているが、データストリームの中に基準信号を挿入することで、（１）と（３）あるいは（２）と（４）の手順を同時に実施することができるといった有利な特長を有することが出来る。

（実施の形態４）

通信相手である端末に対して伝搬状態を制御する方法について図４、図９用いて説明する。また、ここでは通信端末のアンテナ９０１は４つのアンテナ素子（ＡＮ１～ＡＮ４）からなるものとする。

図４における動作は、上記実施の形態２で記述したことと基本的には同一で

ある。ここでは、相違点のみ説明する。

コンボルバ４０３は、夫々の受信信号に対して基準信号を用いて遅延プロファイルを生成し、４種類の遅延プロファイルがバッファ４０４で保持される。ここで、各遅延プロファイルをＤｓ１～Ｄｓ４とする。さらに、受信信号と受信重み付け係数（Ｗｒ１～Ｗｒ４）を用いて、

$$R0 = \Sigma Rm \cdot Wrm \qquad (2)$$

で与えられる受信信号Ｒ０の遅延プロファイル（Ｄｓ０）を計算し出力する。これらの遅延プロファイル（Ｄｓ０～Ｄｓ４）のうち、Ｄｓ０は符号化部１０５へ入力され、暗号鍵Ｋ０、対応コードｍ０が出力される。

なお、受信重み付け係数Ｗｒ１～Ｗｒ４は初期状態などにおいて初期値に設定されるものとする。

このようにして求められたＤｓ１～Ｄｓ４、Ｗｒ１～Ｗｒ４、Ｄｓ０、ｍ０を用いて伝搬制御を行う具体的な方法について図９を用いて説明する。

図９のアンテナ９０１は４つのアンテナ素子で構成され、受信復調部９０２は各アンテナ素子からのＲＦ信号を入力し、各受信信号および受信系列に対応する受信重み付け係数を出力し、伝搬推定部１０３は受信重み付け係数と各受信信号とを入力し、伝搬推定を行い伝搬情報を出力し、符号化部１０５は伝搬情報から特徴を抽出し暗号鍵の対応コードを出力し、伝搬制御部９０９は伝搬情報と暗号鍵の対応コードと、受信重み付け係数とを入力し、送信重み付け係数を出力し、送信変調部９１０は通信情報と送信重み付け係数とから各アンテナに対して送信信号を生成し出力するものである。伝搬制御部９０９は、係数算出部９０３と、コードブック９０５と、バッファ９０４とからなる。係数算出部９０３は伝搬情報と暗号鍵の対応コード、受信重み付け係数、量子化ベクトルを入力して送信信号のアンテナ素子に対応する送信重み付け係数を出力する。

バッファ９０４は送信重み付け係数を保持するものであり、コードブック９０５は対応コードと量子化ベクトルを格納したものである。送信変調部９１０

は、変調部９０６と、重み付け部９０７と、送信部９０８とからなる。変調部９０６は通信情報を入力して所定の変調方式で変調し、変調信号を出力し、重み付け部９０７は変調信号とアンテナ素子に対応した重み付け係数とを乗じて、重み付け変調信号を出力し、送信部９０８はアンテナ素子に対応する重み付け変調信号を入力し、夫々の信号をアンテナ素子に対応するＲＦ信号を出力するものである。

次に、受信装置１０００について、図１０を用いて説明する。

特徴抽出部１００１は、受信信号から得られた伝搬情報を入力しその特徴を抽出する。

バッファ１００２は、抽出した特徴抽出情報を一時記憶しておく。そして、バッファ１００２は、記憶した特徴抽出情報を第１データとして出力する。

図９で説明した各ブロックの機能は、図４、図７に記述された各部位とほぼ同等である。ここでは、相違点のみについて説明する。

アンテナ９０１は４つのアンテナ素子（ＡＮ１～ＡＮ４）から構成されるアンテナであり、受信したＲＦ信号をアンテナ素子毎の４系統出力する。また受信時に用いるアンテナ毎の受信重み付け係数（Ｗｒ１～Ｗｒ４）も同時に出力する。ＡＮ１～ＡＮ４に対応する受信信号（Ｒ１～Ｒ４）は伝搬推定部１０３に入力される。上述の通り、伝搬推定部１０３では各受信信号（Ｒ１～Ｒ４）に対応する伝搬状態（Ｄｓ１～Ｄｓ４）を出力し、符号化部１０５は暗号鍵Ｋ０、対応コードｍ０を出力する。

係数算出部９０３は、暗号鍵Ｋ０に対応するコードｍ０をコードブック９０５で検索し、コードｍ０の対象となっている量子化ベクトル（Ｘｑｍ０）を読み、保持する。量子化ベクトル（Ｘｑｍ０）と入力された伝搬情報（Ｄｓ０～Ｄｓ４）とを用いて、

$$d = |Wm \cdot Dsm - Xqm0|^2 \qquad (3)$$

で与えられる２乗誤差が最小になるようなＷｍ（ｍ：１～４）を求める。この算出法としては最小２乗法などが有名である。

こうして得られた重み付け係数（Ｗ１～Ｗ４）と受信重み付け係数（Ｗｒ１～Ｗｒ４）とを用いて、

Ｗｔｍ＝Ｗｍ／Ｗｒｍ（ｍ：１～４）　　（４）

で与えられる送信重み付け係数（Ｗｔ１～Ｗｔ４）を求め出力する。バッファ９０４は送信重み付け係数を保持する。

一方、通信情報を入力した変調部９０６は、所定の変調方式に従って通信情報を変調し、変調信号を出力する。この変調信号は、アンテナ素子（ＡＮ１～ＡＮ４）に対応する変調信号系統（Ｓ１～Ｓ４）に分岐され、重み付け部９０７へ送出される。重み付け部９０７では、バッファ９０４からの送信重み付け係数（Ｗｔ１～Ｗｔ４）と、ＡＮ１～４に対応した変調信号（Ｓ１～Ｓ４）とを乗じる。

Ｓｗｍ＝Ｗｔｍ・Ｓｍ（ｍ：１～４）　　（５）

こうして得られた重み付け変調信号（Ｓｗ１～Ｓｗ４）を出力する。送信部９０８は、重み付け変調信号を入力し夫々をＲＦ信号（Ｓｒｆ１～Ｓｒｆ４）に変換してアンテナ９０１へ出力する。

以上のような計算を行いながら送信変調部９１０において送信重み付け係数を乗ずることで、受信する端末においてＸｑｍ０で表される伝搬特性の制御が可能となる。

次に、アンテナ９０１から送信された送信信号を受信した受信装置１０００は、伝搬推定部１０３にて受信信号より伝搬状態を推定して、推定した伝搬状態情報を特徴抽出部１００１へ出力する。特徴抽出部１００１は、伝搬状態情報より伝搬状態に応じた特徴を抽出して第１データとして出力する。

このように、本実施の形態４の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、送受信装置９００と受信装置１０００とで同一の第１データを取得することができるように、送受信装置９００は伝搬推定部１０３にて推定した伝搬環境に基づいて通信情報を送信する際の重み付けを調整するので、ノイズ等が伝搬環境を推定する際に影響することにより送受信装

置９００と受信装置１０００とで同一の第１データが取得できなくなるという状態を防ぐことができるとともに、第１データの曖昧さをなくすることができる。また、本実施の形態４の通信装置及び通信システムによれば、送受信装置９００は、伝搬推定部１０３にて推定した伝搬環境に基づいて通信情報を送信する際の重み付けを変えることにより、意図的に受信装置１０００が取得する第１データを変更することができるので、長期間同一の第１データを使うことにより秘匿情報が解読される等の弊害を防ぐことができる。これにより、第１データが暗号鍵である場合には暗号鍵を変更することができるため、高いセキュリティを確保することができる。

なお、本実施の形態４においては、遅延プロファイルを制御するものとして説明したが、これに限らず、偏波状態（偏波面、旋回方向）や、位相状態、伝搬遅延時間を用いて伝搬推定するようにしても良い。また、本実施の形態４においては、コードブック９０５は符号化部１０５が持っているコードブックと同一のものであり、構成上はどちらか一方が在ればよい。また、本実施の形態４においては、アンテナ９０１はアンテナ素子数が４の場合について説明したが、これに限らず、２以上であれば同様の効果が得られることはいうまでもない。また、数式で示した各符号は自然数であっても複素数であっても適用可能である。各値が複素数である場合、信号制御が振幅と位相で行えるため、より高度な制御を期待できる。

（実施の形態５）

本発明の実施の形態５に係る通信装置は、伝搬制御を行うことで、任意の暗号鍵を選択できるものであり、図１１は、本発明に関する通信手順を示したものである。なお、本実施の形態５における通信装置は、図７に記載した通信装置７００と同一構成であるので、その説明は省略する。

上記実施の形態１～４では、推定した伝搬状態に対応する暗号鍵を選択して通信を行うことから、伝搬状態が一定である場合、暗号鍵が長時間の間同一となってしまう。そのため、暗号鍵の推定が容易になってしまう虞がある。また、

両通信装置で同一の暗号鍵を用いるため、一方の暗号鍵が判明した場合、他方の暗号鍵も判明してしまうといった虞がある。本実施の形態５においては、上記実施の形態１～３においては、第１鍵と第２鍵が同一であったものに対して、これを送信者が選択できるところが異なる。

図１１は、本発明に関する通信手順を示したものである。なお、（０）～（４）の手順は図８と同一であるのでその説明は省略する。

（５）基地局：第３基準信号送信

基地局は、暗号鍵として第３鍵を選択しその暗号鍵に対応する伝搬特徴情報と、最後に推定された通信の伝搬情報とから重み付け係数を決定する。次に、伝搬制御部７０１（第２データ選択手段）は、端末で行う伝搬推定用の基準信号を重み付け係数によって伝搬制御を行いながら第３基準信号として出力する。

端末は基地局からの信号を待っており、伝搬推定部２０３は受信した受信信号から第３基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。この推定値である伝搬情報は、符号化部７０３と伝搬制御部７０１へ送出される。符号化部７０３は、伝搬推定部２０３からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴情報を伝搬制御部７０１へ出力する。同時に、抽出した伝搬特徴情報を用いて暗号鍵への変換を行う。変換された暗号鍵はバッファ２０６に保持され暗号鍵情報が出力される。この暗号鍵を第３鍵として基地局は以降の通信の暗号鍵とする。

（６）端末：第４基準信号送信

端末は、（５）と同様に暗号鍵として第４鍵を選択しその暗号鍵に対応する伝搬特徴情報と、最後に推定された通信の伝搬情報とから重み付け係数を決定する。次に、基地局で行う伝搬推定用の基準信号を重み付け係数によって伝搬制御を行いながら第４基準信号として出力する。

基地局では、端末からの信号を受信すると第４基準信号を検出し、伝搬推定部２０３は受信信号と既知信号である基準信号とから伝搬推定を行う。（５）

と同様、伝搬推定部２０３は伝搬情報を出力し、符号化部７０３は伝搬情報から伝搬特徴情報を抽出して出力する。さらに伝搬特徴情報から暗号鍵へと変換され、バッファ部２０６で暗号鍵情報が保持される。この暗号鍵を第４鍵として端末は以降の通信の暗号鍵とする。

（７）基地局：暗号送信

基地局は、（５）で選択した第３鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化信号を送信する。

端末は、暗号化信号を受信すると受信復調部７０８が受信信号を復調情報へと復調する。復号化部２０７は復調情報と（５）で求めた第３鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

（８）端末：暗号送信

端末は、（６）で選択した第４鍵を用いてセキュリティデータを暗号化し、暗号化信号を送信する。

基地局は、（７）と同様に（６）で求めた第４鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

以上の動作について数式を交えて説明する。

電波伝搬の特性を表す伝搬関数Ｈ、受信信号Ｓｒ送信信号Ｓｔを用いて表すと、

$$Sr = H \cdot St \qquad (6)$$

の式が成り立つ。アンテナの素子数をＮとすると、ＨはＮ×Ｎの正方行列、ＳｒとＳｔは１×Ｎの行列である。端末は基地局が送信する信号（図３では第１基準信号）、基地局は端末が送信する信号（図３では第２基準信号）を用いて計算することができる。第１基準信号および第２基準信号の通信を式で表すと、

$$Sr\_b = Hu \cdot St\_m \qquad (7)$$

$$Sr\_m = Hd \cdot St\_b \qquad (8)$$

と表現できる。ＨｕおよびＨｄはアップリンク・ダウンリンクの伝搬関数、Ｓｔ＿ｂ、Ｓｒ＿ｂは基地局側の送受信信号、Ｓｔ＿ｍ、Ｓｒ＿ｍは端末側の送

受信信号である。また、Ｓｔ＿ｂおよびＳｔ＿ｍは既知信号（第１、第２基準信号）であるから、伝搬関数はそれぞれ、

$$Hu = Sr\_b \cdot St\_m^{-1} \quad (9)$$

$$Hd = Sr\_m \cdot St\_m^{-1} \quad (10)$$

で求められる。伝搬関数は伝搬の相反性から、送信時と受信時では同一となることから、

$$H \equiv Hu = Hd \quad (11)$$

である。この様にして得られた伝搬関数Ｈを暗号鍵（第１鍵（＝第２））に用いるのが第１の実施の形態に示したものである。

一方、送信重み付け係数Ｗｂ、Ｗｍを用いて伝搬状態を制御する方法について説明する。暗号鍵（第１鍵（＝第２鍵））を選択する際に求めた量子化ベクトルで示される伝搬関数Ｈ’と実際の伝搬関数Ｈとの間に誤差εが在る場合は、

$$Sr = (H' \cdot \varepsilon) \cdot St \quad (12)$$

で示されるから、誤差成分εは、

$$\varepsilon = H^{-1} \cdot (Sr \cdot St^{-1}) \quad (13)$$

で求めることができる。これを重み付け係数Ｗｍ、Ｗｂに置き換えることで、

$$Sr\_b = (H' \cdot Wm) \cdot St\_m \quad (14)$$

$$Sr\_m = (H' \cdot Wb) \cdot St\_b \quad (15)$$

のように補正が可能である。この様にして重み付け係数を用いて伝搬状態を補正しながら暗号通信を行うのが第４の実施の形態に示したものである。さて、この補正機能をさらに発展することで、暗号鍵を送信側で設定することも可能である。第１鍵（＝第２鍵）とは異なる第３鍵、第４鍵を用いる場合について説明する。基地局は、第３鍵に対応する伝搬関数Ｈ３になるよう重み付け係数Ｗ３＿ｂによって制御を行い、これを第３基準信号を通じて送信する。すなわち、

$$Sr\_m = (H \cdot W3\_b) \cdot St\_b \quad (16)$$

とした場合、

$$H3=H\cdot W3\_b \qquad (17)$$

である。以降基地局は第３鍵を用いて暗号化を行いながら暗号化通信を実施する。

端末は、第３基準信号を受信し伝搬状態を解析することで、伝搬関数Ｈ３を得ることが出来るからそれに対応する暗号鍵（第３鍵）を用いて、以降の暗号化情報を復号していけばよい。同様にして、端末側は第４鍵を選択（対応する伝搬関数はＨ４とする）し、重み付け係数Ｗ４＿ｍによって制御を行いながら第４基準信号を通じて送信する。

$$Sr\_b=(H\cdot W4\_m)\cdot St\_m \qquad (18)$$

$$H4=H\cdot W4\_m \qquad (19)$$

端末は第４鍵を用いて暗号化を行いながら暗号化通信を実施する。同様にして基地局が第４鍵を用いて復号可能である。

このように、本実施の形態５の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、伝搬制御部７０１は基準信号を送信する際に伝搬環境が変化するように送信部７０５と変調部７０４を制御するので、任意のタイミングにて暗号鍵を変更することができるので、第三者により暗号鍵を解読される可能性がなくなり、高いセキュリティを提供することができる。

（実施の形態６）

上記実施の形態１～５において説明したフレーム構成は、図１２（ａ）を基準に説明している。つまり、基準信号を含むバーストと、暗号化信号を含むバーストが別に存在している形態である。この方式を用いると基準信号期間を長く取れるため、受信側の推定誤差を小さくできるといった特長がある。

図１２（ｂ）の場合は、フレーム構成がデータストリーム（或いはバースト）中に所定の期間、基準信号を挿入する方法である。この方式によると、暗号化信号と同時に暗号鍵を授受することが可能であり、効率的な伝送を行うことが出来るようになる。

一方、図１２（ｃ）は、基準信号が示す暗号鍵と暗号化信号が用いる暗号鍵

の配置について示している。図１２（ｃ）に示すように、基準信号が示す暗号鍵と対応するデータ信号との間で時間的（或いは周波数的）に所定の方式に従って変化を付けることで、暗号鍵と対応する暗号化信号とを独立して授受することが可能となるため、第３者へ両者が漏洩する危険性が減るといった特長を有する。

暗号鍵の授受については、他の実施の形態において通信手順にも示した通り、基準信号を用いて行われていることとしている。図１１の（１）、（２）がそれに相当する。図１１では、これ以外の通信では暗号鍵の授受は行われていない。これは、暗号化通信時の伝搬状況には復号動作が左右されないことを示している。つまり、基準信号の送信時は伝搬環境に応じて特徴的な伝搬情報が伝達できるように伝搬制御を行うことで安定した暗号鍵の授受が可能となる。

次に、通信手順と対応する伝搬制御の操作を、図１３を用いて説明する。

まず、図１２（ａ）のフレーム構成における通信について説明する。

図１３の（１ａ）において基準信号が送信される際、伝搬制御は他の実施の形態で述べたように暗号鍵を授受するための通信を行う。この時、以前に伝搬推定を実施していれば、その推定結果と暗号鍵に対応する伝搬状態との差を補正するような制御を行うことが可能である。こうすることで受信側は伝搬状態が良好な状態で基準信号を受信可能であり、安定した暗号鍵授受が行えることになる。一方、図１３の（２ａ）において、データ通信（暗号化信号）を行う場合、暗号鍵は既に受信側に届いており、受信・復号に伝搬情報を用いる必要はない。このため、制御方式としては受信が安定して行えるような制御（ビームフォーミング、送信側の等化、送信ダイバーシチなどが知られている）を行うことでデータ通信を安定して行うことが出来る。以降、図１３の（３ａ）以降の様に通信を行うことで大幅な通信品質の向上が見込める。

次に、図１２のフレーム構成（ｂ）における通信について説明する。

図１３の（１ｂ）に示すように、基準信号通信時とデータ通信時とで伝搬制御方式を切り換えることが考えられる。この方式を用いると、暗号鍵と暗号化

信号とを同時に伝達することが可能である。送信側で暗号を選択できることは既述の通りであるが、その特性を利用することで毎ブロック暗号鍵を変更するといった柔軟な事も可能になる。その上、先に説明したように安定した通信が行えるといった特長がある。

一方、基準信号通信時とデータ通信時の伝搬制御方式を同一にすることも当然可能である。この場合、データ通信時の復調に基準信号を利用することが可能となり、通信品質の向上が見込める。

以上、説明の中で基準信号として既知信号を想定して説明を行った。しかし、基準信号は既知信号である必要はない。この場合、復調しながら伝搬の変化を推定し、暗号鍵を決定する事になる。このようにする事で、暗号鍵を決定するための情報が増加し、安定して暗号鍵の検出が行えるようになる。また、基準信号はＱＡＭ変調などに用いられるパイロット信号、ＴＤＭＡなどで行うバースト同期用の同期信号系列などを用いることも可能であり、このような構成によると、従来構成をほとんど変更せずに高いセキュリティ性を確保した通信が提供できるといった特長がある。

図１２のフレーム構成（ｂ）、（ｃ）のように、データストリームの中に基準信号を挿入することで、図１１の（１）と（３）あるいは図１１の（２）と（４）の手順を同時に実施することができるといった有利な特長を有することが出来る。

以上の説明では、データ通信時の伝搬制御方式をビームフォーミングやプリコーディング（送信側の等化）、送信ダイバーシチなどとしたが、ＭＩＭＯ（Ｍｕｌｔｉ－Ｉｎｐｕｔ　Ｍｕｌｔｉ－Ｏｕｔｐｕｔ）の制御や、空間多重制御（Ｓｐａｃｅ　Ｄｉｖｉｓｉｏｎ　Ｍｕｌｔｉｐｌｅｘｉｎｇ）などを行うことも考えられる。特にＭＩＭＯ多重化技術や空間多重技術は、伝搬特性を積極的に利用してチャネル容量の拡大を図る技術であり、本発明に記述されている技術も伝搬特性を積極的に利用したものであり整合性が良い。例えば、上記実施の形態で示した技術を用いて秘匿通信を行った後、伝搬制御をＭＩＭＯ向け

に（或いは空間多重制御向けに）変更することで引き続き、ＭＩＭＯや空間多重を行うことが可能となる。この様にすることで、特別な技術構成を追加することなく、重要な情報に対しては秘匿性を高くし、データ通信に対してはチャネル容量を向上させることが可能になる。

このように、本実施の形態６の通信装置及び通信システムによれば、上記実施の形態１～５の効果に加えて、通信相手が伝搬環境に基づいて暗号鍵（第１データ）を取得するために送信する信号とそれ以外の信号との送信の際の伝搬環境を変化させるので、通信相手に暗号鍵を取得させるために送信する信号以外の信号を通信環境に応じて最適な制御方式にて送信することができる。

なお、本実施の形態６においては、説明の中で基準信号として既知信号を想定して説明を行った。しかし、基準信号は既知信号である必要はない。この場合、復調しながら伝搬の変化を推定し、暗号鍵を決定する事になる。このようにする事で、暗号鍵を決定するための情報が増加し、安定して暗号鍵の検出が行えるようになる。また、基準信号はＱＡＭ変調などに用いられるパイロット信号、ＴＤＭＡなどで行うバースト同期用の同期信号系列などを用いることも可能であり、このような構成によると、従来構成をほとんど変更せずに高いセキュリティ性を確保した通信が提供できるといった特長がある。

（実施の形態７）

本発明の実施の形態７に係る通信装置は、図１４は、本実施の形態７に係る通信装置における受信装置の一部を示すものであり、図１５は、本実施の形態７に係る通信装置における送信装置の一部を示すものである。なお、上記実施の形態１における通信装置と同一構成である部分は同一の符号を付して、その説明は省略する。

ここでは、多重した信号への適用方法について説明する。多重アクセス方式としてはＣＤＭＡを例に挙げる。

受信復調部１５０は、ＲＦ信号を受信した受信信号と復調した復調情報とを出力する。受信復調部１５０は受信部１４０１、逆拡散部１４０２、伝搬推定

部１４０５、復調部１４０３とからなる。

図１４は本発明に供する受信装置の一部を示したものである。

受信部１４０１は、ＲＦ信号と伝搬情報を入力し、ＲＦ信号を適切な受信状態に制御し、受信信号を出力し、逆拡散部１４０２は受信信号とチャネルに対応する拡散符号との畳み込み積分を行い逆拡散信号を出力し、復調部１４０３は、受信信号と伝搬情報とから適切な復調を行い復調情報を出力し、復号化部１４０４は、暗号鍵情報と復調情報とを入力し、暗号鍵情報から復調情報の暗号を復号化しセキュリティデータを出力し、伝搬推定部１４０５は各チャネルの伝搬推定をおこない各チャネルに対しての伝搬情報を出力し、復調部１４０３は、受信信号と伝搬情報とから適切な復調を行い復調情報を出力し、比較部１４０６はチャネル毎の伝搬情報を比較し比較結果（第１データ）を出力し、暗号鍵生成部１４０７は、伝搬情報を入力し暗号鍵情報（第１データ）を出力する。

図１５は本発明に供する送信装置の一部を示したものである。

データ供給部１５０１、１５０２はチャネル毎のデータを保持し、変調拡散部１５０３、１５０４はチャネル毎のデータを変調しチャネルに対応する拡散符号で拡散して、拡散信号を出力し、重み付け部１５０５は送信信号と送信重み付け係数を乗じ、送信部１５０６は、変調信号を送信するＲＦ信号に変換して出力し、アンテナ１５０７は、送信信号を送信し、データ供給部１５０８は第１データを格納し、基準伝搬バッファ１５０９は伝搬状態の基準情報を保持し、伝搬制御部１５１０は暗号鍵と第２データと伝搬情報とを入力し送信重み付け係数を算出する。

次に、送信装置１５００の動作について説明する。

送信装置１５００は、データ供給部１５０１、１５０２から複数チャネル分のデータを取りだし夫々を変調し、予め設定されている拡散符号を用いて各チャネルの拡散信号を生成する。データ供給部１５０８は第１データを出力し、

それを入力した伝搬制御部１５１０は、事前に推定された伝搬情報が保持された基準伝搬バッファ１５０９からの情報を基に、第１データに対応する伝搬状態制御を、送信重み付け係数によって行う。送信重み付け係数は重み付け部１５０５で重み付け演算が行われ、送信部１５０６を通じて送信される。

まず、簡単のためデータ供給部１５０８からの出力がないものとする。伝搬制御部１５１０の制御自体は図７で示した伝搬制御部７０１と同一である。例えば、チャネルが１つである場合は実施の形態４でしめした基準信号を出力している状態と一致する。チャネルが複数ある場合を考える。拡散符号はチャネル毎に設定されているが、各符号間の相関はないため、信号処理上ではそれぞれが独立に処理されていることと同義となる。則ち、伝搬制御部１５１０はチャネル数をM、アンテナ数をNとするとM×N個以上の送信重み付け係数によってチャネル毎に伝搬制御が行えることになる。

以上説明した通り、上記実施の形態５同様に暗号鍵に応じた伝搬制御が行えることが分かる。

さて、複数チャネルが多重されている場合、チャネル毎に伝搬制御を行うことにより、受信端での受信電力を制御することも可能である。例えば、暗号鍵の状態に応じて、どのチャネルが最大電力とするかを制御できることになり、このチャネル番号と受信電力の関係によって受信装置は暗号鍵を決定することが可能となる。さらに、上述のとおり、伝搬パラメータとして（例えば遅延プロファイル）を設定できるので、例えば遅延プロファイルに暗号鍵情報を、チャネルと受信電力の関係に第１データを利用すること（或いは逆でも構わないし、暗号鍵情報だけ、第２データだけといったことも可能である）によって、より多くのセキュアな情報を送信することが可能であることがわかる。

さらに、データ供給部１５０１、１５０２に格納されたデータのうち、１つを基準信号とすることも可能である。この様にすることで、受信装置は第１データや第２データと同時刻に基準信号による伝搬推定の実施が可能になるので、非常に効率の高い伝送が可能になるといった特長を有する。

次に、受信装置の動作について説明する。

伝搬パラメータ（遅延プロファイルなど）を用いて暗号鍵情報を授受する方法については、逆拡散処理を除き上述のものと同一に行うことが可能である。ここでは、多重化されたチャネルと受信電力の関係に情報が重畳されている場合についてのみ説明を行う。

アンテナ１０１から入力されたＲＦ信号は受信部１４０１で受信され受信信号が出力される。受信信号は逆拡散部１４０２において、チャネル毎に予め設定された拡散符号とで畳み込み演算が施され、逆拡散信号がチャネル数分出力される。これら逆拡散信号は、伝搬推定部１４０５へ入力され伝搬状態が推定される。ここでは伝搬状態のうち、受信電力を用いるものとする。伝搬推定部１４０５からチャネル毎の受信電力が出力されると、比較部１４０６によって受信電力の比較が行われ、この結果を暗号鍵情報（或いは第１データ）として出力する。

この様にして決定された暗号鍵を用いて、復号化部１４０４は以降の復調情報を復号化し、セキュリティデータを得る。

このように、本実施の形態７の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、比較部１４０６は、多重された受信信号において、各チャネルの信号の受信電力等の伝搬パラメータの比較結果を情報として送ることができるので、多重信号を送信する場合における情報量を増やすことができる。また、本実施の形態７の通信装置及び通信システムによれば、複数チャネルを多重する場合、チャネル毎に伝搬制御を行うことにより、受信端での受信電力を制御することも可能であり、例えば、暗号鍵の状態に応じて、どのチャネルが最大電力とするかを制御できることになり、このチャネル番号と受信電力の関係によって受信装置は暗号鍵を決定することが可能になるので、複数チャネルのデータのセキュリティを維持することができる。また、本実施の形態７の通信装置及び通信システムによれば、第１データにおける遅延プロファイルのような伝搬パラメータに暗号鍵情報を含めるとともに、チャネルと受

信電力との関係を用いて第１データとは異なる情報の第２データとすることができるので、より多くのセキュアな情報を送信することが可能になる。

なお、本実施の形態７において、ＣＤＭＡを例に挙げたがＯＦＤＭでも同様の効果が得られることはいうまでもない。ＯＦＤＭとなる場合、上記説明におけるチャネルをサブキャリアとし、図１４の逆拡散部処理はフーリエ変換処理に、図１５の拡散処理は逆フーリエ変換処理に置き換えることで可能である。

（実施の形態８）

図１６は、本実施の形態８に係る通信装置の一部の構成を示す図である。なお、通信装置全体の構成は図１と同一構成であるのでその説明は省略する。

本実施の形態８は、伝搬情報として受信到来方向情報を利用した方式について説明する。到来方向推定を行う際の構成を、図７の伝搬推定部２０３の詳細ブロック図を図１６に示す。

伝搬推定部２０３は、バッファ１６０１、相関行列演算部１６０２、行列演算部１６０３、角度スペクトラム演算部１６０４、バッファ１６０５で構成されている。

バッファ１６０１は、入力信号を一時保持し、相関行列演算部１６０２は入力信号の相関行列を求め、行列演算部１６０３は計算された相関行列を入力し行列演算（ここでは固有ベクトル）で求めた固有ベクトルを出力し、角度スペクトラム演算部１６０４は、固有ベクトルを入力して角度スペクトラム演算し到来方向推定情報を出力し、バッファ１６０５は演算結果を一時保持する。

以上の構成は到来方向推定法として知られているＭＵＳＩＣ法を用いている。他に、フーリエ法やＣＡＭＥ法が知られているが、これは行列演算部１６０３の演算内容によって分類される。

以上の構成において、伝搬推定部２０３が伝搬情報として到来方向推定を行う際の動作について詳細に説明する。

複数のアンテナ素子から入力された受信信号は、バッファ１６０１において保持される。保持された受信信号は相関行列演算部１６０２においてその相関

行列が求められ、次に行列演算部１６０３において固有ベクトルが算出される。角度スペクトラム演算部１６０４は固有ベクトルから、受信信号到来パターン情報を算出しこれを出力する。この様にして得られた受信信号到来パターン情報はバッファ１６０５で保持される。この様にして求められる受信信号の到来方向情報の一例を図１７に示す。図１７では信号の到来方向が２つ存在する場合の推定結果を示している。

この様にして得られた受信信号の到来パターン情報を用いて、図１１に示す手順で説明を行う。なお、本実施の形態６の動作において、上記実施の形態５と相違する部分についてのみ説明する。

（１）基地局：第１基準信号送信

基地局は、端末の伝搬推定用に第１基準信号を送信する。この時、複数のアンテナ素子によるビームステアリングを行って、放射パターンを変化させながら送信する。

端末は、基地局が出力する基準信号を検出すると、伝搬推定部２０３は、到来方向推定を行い、基地局が制御する放射方向と、端末における受信信号到来パターン情報との対比データを参照テーブル上に格納する。以上の操作により、基地局と端末との間における放射パターンと受信到来パターンとの参照テーブルができあがる。

（２）端末：第２基準信号送信

端末は、暗号鍵（第１鍵）を選択し、コードブックからそれに対応する到来方向情報を出力する。この到来方向情報を、参照テーブルに格納されている放射パターンに最も類似しているものを検出し、これに対応する到来パターン情報を出力時の放射パターンとして設定する。次に、基地局の伝搬推定用に第２基準信号を、設定した放射パターンになるよう制御しながら送信する。

基地局は、伝搬推定部２０３で到来方向推定を行い受信到来パターンを出力する。符号化部７０３は受信到来パターンとコードブックから暗号鍵（第２鍵）を選択し、バッファ２０６を介して復号化部２０７へ出力する。

（３）基地局：暗号化信号送信

基地局は、（２）で求めた受信到来パターンから、端末の受信状態が良好になるような放射パターンに設定する。次に第２鍵を用いてセキュリティデータを暗号化し、設定した放射パターンになるよう制御しながら暗号化信号を送信する。

端末は、ＲＦ信号を受信復調部７０８で復調し、復号化部２０７で第１鍵を用いて復号化し、セキュリティデータを出力する。

（４）端末：暗号化信号送信

端末は、（１）で求めた受信到来パターンから、基地局の受信状態が良好になるような放射パターンに設定する。次に、セキュリティデータを第１鍵で暗号化させながら設定した放射パターンになるように制御しながら暗号化信号を送信する。

基地局は、ＲＦ信号を受信復調部７０８で復調し、復号化部２０７で第２鍵を用いて復号化し、セキュリティデータを出力する。

このように、本実施の形態８の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、角度スペクトラム演算部１６０４は、受信信号の到来方向推定結果を伝搬環境の推定値として用いるので、第３者に到達する受信到来パターンは大きく変化するため、非常に高いセキュリティを確保出来る。

なお、本実施の形態８において、受信到来パターンを用いて暗号鍵情報を作成することとしたが、これに限らず、伝搬情報として遅延プロファイルを用いる方式と組み合わせることで、一層高いセキュリティが期待できるといった特長を有する。また、本実施の形態６において、受信信号の到来方向に情報を重畳することや、到来方向に対して通信の多重化を行うことも可能である。また、通信手順はここで説明したものに限られるものではない事は、他の実施の形態で述べたことと同じである。

（実施の形態９）

本実施の形態９においては、偏波を応用したセキュリティ通信方式について

説明する。

図１８は、本実施の形態９に係る通信装置である送受信装置１８００の構成を示す図である。なお、図１８において、図２と同一構成である部分には同一の符号を付してその説明は省略する。

アンテナ部１８１２は垂直偏波アンテナ１８０１と水平偏波アンテナ１８０２からなり、伝搬推定部２０３は、位相差検出部１８０３と電界強度検出部１８０４と偏波推定部１８０５からなり、偏波制御部１８１３は係数算出部１８０６とコードブック１８０７とバッファ部１８０８からなり、送信変調部２５２は変調部１８０９と重み付け部１８１０と送信部１８１１とからなる。

垂直偏波アンテナ１８０１は垂直偏波成分を受信し、水平偏波アンテナ１８０２は水平偏波成分を受信し、位相差検出部１８０３は両偏波受信信号から位相差を検出し、電界強度検出部１８０４は垂直偏波受信信号と水平偏波受信信号とから夫々の電界強度を検出し、偏波推定部１８０５は位相差と電界強度から偏波状態を推定する。係数算出部１８０６は伝搬情報とコードブックで示される偏波コードとを入力し垂直偏波送信信号と水平偏波送信信号との位相差制御と電界強度制御を行って送信信号の偏波制御を行う係数を算出し、コードブック１８０７は、係数と偏波コードとの関係を記憶し、バッファ部１８０８は、係数算出部１８０６から入力したデータを一時的に保持して重み付け部１８１０へ出力する。

変調部１８０９は、通信情報を入力して所定の変調方式で変調し、変調信号を出力する。

重み付け部１８１０は、変調信号とアンテナ素子に対応した重み付け係数とを乗じて、重み付け変調信号を出力する。

送信部１８１１は、アンテナ素子に対応する重み付け変調信号を入力し、夫々の信号をアンテナ素子に対応するＲＦ信号を出力する。

次に、送受信装置１８００の動作について説明する。

垂直偏波アンテナ１８０１と水平偏波アンテナ１８０２は受信信号の各偏

波成分を選択的に受信し、ＲＦ信号を受信復調部２５０へ送出する。受信復調部２５０は各偏波に対応する受信信号を出力し、これら受信信号は伝搬推定部２０３へ入力される。伝搬推定部２０３では、位相差検出部１８０３と電界強度検出部１８０４から出力される受信位相差情報と受信電界強度情報が偏波推定部１８０５に入力され、受信信号の偏波情報が出力される。

図１９に偏波状態の具体例を示す。Ｅｖが垂直偏波の電界強度、Ｅｈが水平偏波の電界強度、ｐが旋回方向、θが長軸角度を表している。

このようにして求められた偏波情報は符号化部２０５によって偏波コードに符号化され、暗号鍵が選択される。この偏波コードは偏波制御部１８１３に入力される。偏波制御部１８１３では、係数算出部１８０６がコードブック１８０７から偏波コードに対応する偏波状態を検索し、位相制御や電界強度制御などを行いながら送信重み付け係数を算出し、バッファ部１８０８に保持する。バッファ１８０８に保持された送信重み付け係数は、送信変調部２５２によって垂直偏波送信信号と水平送信偏波信号とがそれぞれ重み付けされ、ＲＦ信号として対応するアンテナ素子から出力される。

以上のような操作を行うことで、例えば垂直偏波、水平偏波であるとか、長軸の角度、偏波間の位相、旋回方向などが暗号鍵として用いることが可能となる。

伝搬状態のなかで、偏波はアンテナに依ってのみ分離されるという特長がある。

なお、コードブック１８０７の量子化ベクトルの内容としては、偏波状態（偏波面や旋回方向など）に対応するものが格納されているものとする。通信手順については、他の実施の形態で示したものとほぼ同じである。遅延プロファイルの検出、あるいは伝搬制御の箇所が、夫々偏波情報や偏波制御に置き換わるものである。

このように、本実施の形態９の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、偏波推定部１８０５は、電界強度と位相差から偏波状態を推定して伝搬環境の推定値とするので、偏波はアンテナに依ってのみ

分離されるという特長があるため、他の受信装置が電波を傍受したとしても、アンテナが対応してなくてはならないことを意味し、高いセキュリティが期待できる。

なお、本実施の形態９においては、伝搬状態として遅延プロファイルや受信パワー、到来方向パターンなどと併用することも可能である。

（実施の形態１０）

上記実施の形態１～９に記載の方式に加え、受信端末における通信状態を制御し、その制御状態に対して情報を重畳させる方式を用いて、第３者における傍受を原理的に不可能にする方式について説明を行う。

実施の形態５において、受信側における伝搬状態を任意に制御できることを示したが、この方式を用いることで物理的に秘匿性のある通信が可能になる。このことを簡単に説明する。

上述した実施の形態５の例では、送信信号の重み付け係数によって伝搬状態を制御できることを示した。このことは、受信側に対して任意の受信状態を伝達していることと同義であり、則ち伝搬パラメータを通じて通信が行えることを意味する。

換言すれば、図５に示すようなコードブックの内容（図中では暗号鍵となっているもの）を情報に置き換えることで、伝搬パラメータを通して通信が可能になることを示唆する。

この方法を用いた通信は、別途説明したとおり通信者間で形成される伝搬環境をベースとした通信であるため、原理的に物理的位置が異なる装置に対しては高い秘匿性を有するといった特長がある。また、逆に伝搬パラメータを利用することで、伝搬経路すなわち通信相手の場所を特定していることになり、通信相手の特定や認証にも応用可能である。

また、従来利用されてきた、変調方式（ＡＳＭ、ＦＳＫ、ＰＳＫ、ＱＡＭなど）に依らず適用可能であり、この場合純粋にデータ容量の増加が見込める。

さらに、多重化方式（ＴＤＭＡ、ＦＤＭＡ、ＣＤＭＡ、ＯＦＤＭなど）など

の縦断に依らず適用可能であるといった大きな特長を有する。本方式は、空間の直交性を利用した多重化も可能である。つまり、空間直交性による多重化方式と上記多重化方式を組み合わせることで、従来のチャネル要領を大幅に増加させることが出来るといった効果も期待できる。

また、他の実施の形態で示した暗号化、復号化の処理は特にそれを必要としない装置であれば、必須のものではなくそれがなくても動作することは明白である。

また、他の実施の形態で示した手順の中で暗号鍵情報を送信する必要がない際は、伝搬制御を通信に最適に制御（例えばマルチパス成分を除去したり、受信電力が最大になるよう制御したり）することで通信品質の向上が見込める。

さらに、受信時においても受信信号が受信重み付け係数を用いて最適に制御（上記と同様）する事で、同様に通信品質の向上が見込める。

次に、本実施の形態１０における受信装置の構成について、図２０を用いて説明する。

図２０は、本実施の形態１０に係る通信装置である受信装置２０００の構成を示す図である。なお、図１と同一構成である部分には同一の符号を付してその説明は省略する。

伝搬推定部１０３は、受信部１０２から入力した受信信号から伝搬特性を推定し、推定した伝搬情報をデータとして出力する。伝搬推定部１０３から出力される伝搬情報は、復調部１０４から出力されるデータを破棄するか否かの情報等である。

伝搬特性を通信情報として出力するような受信装置の場合、図２０に示すような構成で実現可能であり送信部は必ずしも必要ではない。この様に構成することで、伝搬情報を第１データとして秘匿性の高い情報として用いることが可能となる。この場合、送信装置では、第１データに重要な重畳することも考えられる他に、この第１データを用いて通信信号を送信した端末の特定に利用することが可能となる。

このように、本実施の形態１０の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、伝搬推定部１０３は、伝搬推定情報をデータとして使用するので、送信する情報量を多くすることができて伝送効率が向上するとともに、秘匿性の高い情報は伝搬情報として送信することができるので、確実なセキュリティを確保することができる。また、本実施の形態１０の通信装置及び通信システムによれば、秘匿性の高くない情報は従来の通信方式により送信することができるので、汎用性のある通信装置を提供することができる。

（実施の形態１１）

図２１は、本実施の形態１１に係る通信装置である受信装置２１００の構成を示す図である。なお、図１と同一構成である部分には同一の符号を付してその説明は省略する。

符号化部１０５は、伝搬推定部１０３から入力した伝搬推定情報を符号化して第１データとして出力する。この推定した伝搬情報を符号化する技術として、ベクトル量子化法などを用いて符号化し、それを伝送情報として出力することも可能であり、この様にすることで多様なパラメータ入力に対して、簡易で安定した符号出力が可能であるという特長がある。

このように、本実施の形態１１の通信装置及び通信システムによれば、上記実施の形態１及び実施の形態１０の効果に加えて、符号化部１０５は、伝搬情報を符号化してデータとして取り出すので、通信品質の向上が見込める。

（実施の形態１２）

図２２は、本実施の形態１２に係る通信装置である受信装置２２００の構成を示す図である。なお、図２２において、図１と同一構成である部分には同一の符号を付してその説明は省略する。

逆拡散部２２０１は、受信信号とチャネルに対応する拡散符号との畳み込み積分を行って逆拡散信号を出力する。

比較部２２０２は、チャネル毎の伝搬情報を符号化し、符号化した各チャネルの伝搬情報を比較し比較結果を第１データとして出力する。

このように、本実施の形態１２の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、比較部２２０２は、複数チャネルのデータを比較し、その比較結果より第１データを取り出すので、秘匿性が高まると同時により多くのデータを伝送出来るといった特長を有する。

なお、本実施の形態１２においては、逆拡散部を設けることによりＣＤＭ信号を用いてデータを取り出すこととしたが、これに限らず、直交周波数分割多重処理された信号を受信して各サブキャリアに配置された信号同士を比較することによりデータを取り出すようにしても良い。また、本実施の形態１２の通信装置は、時空間分割多重（ＭＩＭＯ）信号等を用いて通信を行う場合にも適用可能である。

（実施の形態１３）

本実施の形態１３において、図２３は、受信装置２３００を示す図であり、図２４は、送受信装置２４００を示す図である。なお、図１の受信装置１００及び図２の送受信装置２００と同一構成である部分は同一の符号を付してその説明は省略する。

最初に、受信装置２３００について説明する。

受信復調部１５０は受信したＲＦ信号を入力し推定した伝搬情報と復調した復調信号を出力する。符号化部１０５は伝搬情報を入力しその特徴を抽出しその伝搬特徴符号（第１データ）を出力し、復号化部１０７は伝搬情報の特徴を示す符号と復調信号とを入力し、伝搬特徴符号に対応するインタリーブパターンを用いて順序の逆変換（デインタリーブ）、ヌル情報の追加（デパンクチャ）、復号化（デコード）し、セキュリティデータ（第２データ）を出力し、復調信号を入力し伝搬特徴符号に対応するインタリーブパターンに基づきデータ順序の逆変換を行うデインタリーバ２３０１と、デインタリーブ信号を入力し伝搬特徴符号に対応するパンクチャパターンに基づき除去された箇所の信号に対して（後段のデコーダにとって符号を判断するのに）中立な情報を付加するデパンクチャ部２３０２と、デパンクチャ信号を入力し伝搬特徴符号に

対応する畳み込み符号に対応して復号化するデコーダ２３０３とからなる。

次に、送受信装置２４００について説明する。

受信復調部２５０は受信したＲＦ信号を入力し、伝搬状態を推定した伝搬情報と、復調した復調情報とを出力する。復号化部２０７は伝搬情報の特徴を示す符号と復調信号とを入力し、伝搬特徴符号に対応するインタリーブパターンを用いて順序の逆変換（デインタリーブ）、ヌル情報の追加（デパンクチャ）、復号化（デコード）し、データを出力し、復調信号を入力し伝搬特徴符号に対応するインタリーブパターンに基づきデータ順序の逆変換を行うデインタリーバ２４０１と、デインタリーブ信号を入力し伝搬特徴符号に対応するパンクチャパターンに基づき除去された箇所の信号に対して（後段のデコーダにとって符号を判断するのに）中立な情報を付加するデパンクチャ部２４０２と、デパンクチャ信号を入力し伝搬特徴符号に対応する畳み込み符号に対応して復号化するデコーダ部２４０３とからなる。符号化部２０５は伝搬情報を入力しその特徴を抽出しその伝搬特徴符号（第１データ）を出力し、伝搬制御部２４０４は伝搬状態を入力した伝搬特徴符号に近づけるよう制御する送信重み付け係数を出力し、符号化部２０５はデータを入力するものであり、符号化（エンコード）し、情報の除去（パンクチャ）、順序変換（インタリーブ）した符号化情報を出力し、データを入力し畳み込み符号を出力するエンコーダ２４０５と、畳み込み符号を入力しその符号の一部を除去したパンクチャ符号を出力するパンクチャ部２４０６と、パンクチャ符号の順序を所定の順に並べ替え符号化情報を出力するインタリーバ２４０７とからなる。送信変調部２４１０は符号化情報を入力し、変調して伝搬制御し送信するＲＦ信号を出力するものであり、符号化情報を入力し所定の変調を施し変調信号を出力する変調部２１１と、変調信号を入力し重み付け係数を乗ずることで伝搬制御を行う送信ウェイト部２４０８と、送信ウェイト信号を入力し送信するＲＦ信号を出力する送信部２１２とからなる。

次に、送受信装置２４００の動作について、図２５を用いて説明する。ここ

では、送受信装置２４００が図２５中の基地局と端末であるものとして説明を行う。なお、本実施の形態１３において、端末は送受信装置２４００の構成である場合に限らず、受信装置２３００の構成を有していても良い。

本実施の形態１３における送受信装置２４００の動作において、図３と同一の動作である部分の説明は省略する。

まず、予め伝搬状態に対応するインタリーブパターンや、パンクチャパターン、エンコードパターンを用意しておき、基地局、端末でこの情報を共有しておく。

次に、端末は基地局が送信する基準信号により伝搬状態を推定し、これに基づく各種パターンを設定する。基地局も同様に端末から送信される基準信号により伝搬状態を推定し各種パターンを設定する。この時、設定されるインタリーブパターン、パンクチャパターン、エンコードパターンが基地局、端末と同一のものが選択されることは前述の通りである。

以上の様にして、両者の符号化パターンが設定されると次に両者の間で通信を開始する。基地局は、符号化パターンに基づきエンコーダ部２４０５によって畳み込み符号化が行われ、パンクチャ部２４０６によってパンクチャリングが行われ、インタリーバ２４０７によってインタリービングが行われ、こうして得られた符号化情報が送信変調部２４１０へ送出され、符号化部２０５が出力する伝搬特徴符号は、伝搬制御部２４０４に入力され送信重み付け係数が出力され、送信部２１２によってＲＦ信号が出力、放射される。送信重み付け係数の算出については、実施の形態３で示したようなものと同一である。

端末では、基地局からの信号を受信し、これを受信復調部２５０が受信し、伝搬推定、復調を行い、伝搬情報と復調信号を出力する。復号化部２０７では入力された伝搬特徴符号に基づき、インタリーブパターン、パンクチャパターン、エンコードパターンが選択されている。復号化部２０７は、伝搬特徴符号と、復調信号とを入力し、デインタリーバ２４０１では対応するインタリーブパターンの逆に対応した順序逆変換（デインタリービング）を行い、デインタ

リーブ信号を出力する。デインタリーブ信号はデパンクチャ部２４０２に入力されパンクチャパターンに対応する箇所にヌル信号（後段にあるデコードの際、判断に中立な値）を挿入（デパンクチャリング）したデパンクチャ信号を出力する。デパンクチャ信号はデコーダ部２４０３に入力されエンコードパターンに基づき復号（デコード）を行い、データを出力する。

送信側と受信側において各種符号化パターンを共有していることは前述の通りであり、このため基地局が送信するデータは端末で正常に伝送されることが分かる。

（０）は図３と同一の動作である。

（１）基地局：第１基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第１基準信号として出力する。端末では、基地局からの信号を待っており、伝搬推定部２０３は受信した受信信号から第１基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。符号化部２０５は、伝搬推定部２０３からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴符号を出力する。デインタリーバ２４０１、デパンクチャ部２４０２、デコーダ部２４０３はそれぞれ伝搬特徴符号とインタリーブパターンのテーブル、パンクチャパターンのテーブル、エンコードパターンのテーブルを持っており、入力された伝搬特徴符号から対応する各種パターン（符号化パターン）を選択する。

（２）端末：第２基準信号送信

端末は、（１）と同様に基地局で行う伝搬推定用の基準信号を第２基準信号として出力する。

基地局では、端末からの信号を受信すると第２基準信号を検出し、伝搬推定部２０３は受信信号と既知信号である基準信号とから伝搬推定を行う。（１）と同様、伝搬推定部２０３が出力する伝搬情報は、符号化部２０５によって伝搬特徴符号へと変換され、復号化部２０７で伝搬特徴符号に対応した符号化パターンが選択される。

（３）基地局：符号化信号送信

基地局において、符号化部２４０９は（２）で得られた符号化パラメータを用いてデータのエンコード、パンクチャ、インタリーブした符号化情報を出力する。符号化情報は送信変調部２４１０へと出力され、それらを変調部２１１、送信ウェイト部２４０８、送信部２１２を通じてＲＦ信号が符号化信号として出力される。

端末は、符号化信号を受信すると受信復調部２５０が受信部２０２、復調部２０４を通じてＲＦ信号を復調信号へと復調する。復号化部２０７は復調信号と（１）で求めた符号化パラメータを用い、デインタリーブ、デパンクチャ、デコードの順に復号を行い、データを出力する。

（４）端末：符号化信号送信

端末において、符号化部２４０９は（１）で得られた符号化パラメータを用いてデータのエンコード、パンクチャ、インタリーブした符号化情報を出力する。符号化情報は送信変調部２４１０へと出力され、それらを変調部２１１、送信ウェイト部２４０８、送信部２１２を通じてＲＦ信号が符号化信号として出力される。

基地局は、符号化信号を受信すると受信復調部２５０が受信部２０２、復調部２０４を通じてＲＦ信号を復調信号へと復調する。復号化部２０７は復調信号と（２）で求めた符号化パラメータを用い、デインタリーブ、デパンクチャ、デコードの順に復号を行い、データを出力する。以上のように通信を行うことでデータの授受が行えることが分かる。

このように、本実施の形態１３の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、符号化部２０５は、伝搬環境の推定値よりインタリーブパターンやパンクチャパターン等の制御情報を符号化して求め、求めた制御情報を用いてデータを復号化するので、伝搬状態に応じた最適な符号（復号）が可能となるため、通信品質の向上が見込める。また、本実施の形態１３の通信装置及び通信システムによれば、従来のように符号化パラメータを

通信上でのやりとり（ハンドシェイク）によって授受する必要がなくなり、効率的な上に伝搬環境に素早く対応できるといった大きな特長を持つ。

なお、本実施の形態１３において、符号化パラメータを伝搬状態に応じて変化させて通信を行うもの及び送信時に伝搬制御を行うものとして説明を行ったが、これに限らず、他の実施の形態でも示されているとおり、これは必須ではなく、伝搬制御を行わずに送信する等の任意の方法を採用することができる。また、本実施の形態１３において、符号化方式として畳み込み符号を用いる旨説明したが、これに限らず、ブロック符号等の任意の符号化方式が採用できる。

また、本実施の形態１３において、符号パラメータとしては、エンコードパターン、パンクチャパターン、インタリーブパターンなどを伝搬状態に応じて変化させることとしたが、これに限らず、エンコードパターン、パンクチャパターン、インタリーブパターンの内の一部は固定して用いても良い。こうすることで符号部・復号部をより簡易に構成することが可能である。この場合、通信品質の向上に最も効果的なものを選択することが重要であるが、例えばパンクチャパターンはデータ容量とエラーレートを大きく左右する重要なパラメータの１つであり、このパターンの変更は最も効果的である事が多い。また、本実施の形態９において、図２５の（１）と（２）の手順、あるいは（３）と（４）の手順は前後しても構わないことは明白である。

また、基準信号の授受の後に符号化信号の授受を行っているが、例えば基準信号と符号化信号とを同一のフォーマット上に配し、符号化パラメータの選択した後に復号（あるいは符号）を行うような手順としても構わない。この様にデータと符号化パラメータ推定用の基準信号をセットとすることで、より細かな符号化パラメータの選択が可能となるといった特長がある。

さらに、以上の説明において伝搬パラメータに応じて最適な符号化パラメータを変化させる方法について示したが、符号化パラメータのみではなく、変調方式自体（ＱＰＳＫ、１６ＱＡＭ）や、ＣＤＭＡなどの拡散符号長も変化させることが可能であることは明白である。この様にすることで、符号化パラメー

タ同様柔軟性に富み、さらに効率野よい通信が提供できるといった有利な特長を備える。

（実施の形態１４）

上記実施の形態では、主に伝搬状態を用いたデータ通信について説明を行った。これらは、伝搬状態の推定精度が要求されるといった問題を有している。一般に、推定精度は演算に用いるデータ量に比例するが、データ量が多くなると効率が低下する。また、伝搬推定結果は伝搬推定に用いる基準信号の自己相関にも影響を受ける。これらを解決する手段について、図２６を用いて説明する。

図２６は、受信装置２６００の構成を示す図であり、図２７は、伝搬推定部１０３の構成を示す図である。なお、図１及び図４と同一構成である部分には同一の符号付してその説明を省略する。

最初に、受信装置２６００について説明する。

受信部１０２、伝搬推定部１０３、等化部２６０２及び復調部２６０３は、受信・復調部２６０４を構成する。

等化部２６０２及び復調部２６０３は、等化復調部２６０５を構成する。

符号化部２６０１は、入力された伝搬情報から特長を抽出し、伝搬特長符号（第１データ）を出力する。

等化部２６０２は、推定された伝搬情報と、その特徴を示す伝搬特徴符号とを入力し、受信信号から不要成分の除去を行った等化信号を出力する。

復調部２６０３は、等化信号を入力しそれを復調した結果の復調情報（第２データ）を出力する。

次に、伝搬推定部１０３について説明する。

自己相関部２７０１は基準信号系列を入力しその系列の自己相関関数を出力し、成分除去部２７０２は１次遅延プロファイルをと自己相関関数を入力し、１次遅延プロファイルから自己相関関数成分を除去した２次遅延プロファイルを出力するものであり、平均化演算部２７０３は２次遅延プロファイルを入

力し一定期間の推定結果の平均かを施すものである。

次に、受信装置２６００の動作について説明する。

基本的動作は図１と変わらないため、相違点のみ説明する。入力されたＲＦ信号が受信部１０２により出力された受信信号は、伝搬推定部１０３によって伝搬状態が推定される。この情報は、受信部１０２、等化復調部２６０５、符号化部２６０１へ入力される。符号化部２６０１では入力された伝搬情報から特長を抽出し、伝搬特長符号を出力、この結果が等化復調部２６０５へと入力される。等化部２６０２は推定された伝搬情報と、その特長を示す伝搬特徴符号とを入力し、受信信号から不要成分の除去を行った等化信号を出力する。復調部２６０３は、同様に伝搬情報と伝搬特徴符号とから適した復調手段を用いて等化信号を復調、復調情報を出力する。

この様に、伝搬情報、伝搬特徴符号を等化復調部２６０５に入力し、等化あるいは復調に用いることで、それらを有効に利用して効果的な等化・復調が可能になり、結果として通信品質の向上が見込めるといった特長を有する。

とくに、受信信号から不要成分（たとえばマルチパス成分など）を除去する等化部２６０２に、伝搬特徴符号に対応するタップ係数のテーブルを用意しておき、前記符号に対応したタップ係数を用いて等化処理を行うことで、演算量の大幅な削減効果が得られるといった大きな特長がある。その後、伝搬特徴符号と伝搬情報の差分について等化処理を行うことでより簡易な等化処理部の構成が簡単になるといった特長を有する。

次に、伝搬推定部１０３の動作について説明する。

入力された受信信号を一時保持し、これと基準信号系列とがコンボルバ４０３によって相関値が演算され１次遅延プロファイルが出力される。基準信号系列は、自己相関部２７０１によって自己相関関数が演算されこれが出力される。

遅延プロファイルの演算は

$$Ds(t)=\Sigma(Sr(t+n)\cdot R(n)) \qquad (20)$$

ここで、Ｄｓが推定した遅延プロファイル、Ｓｒは受信信号、Ｒは基準信号系

列である。この時、受信信号は送信信号Ｓｔと伝搬歪Ｐｄを用いて

$$Sr(t)=\Sigma(St(t-n)\cdot Pd(n))$$

$$=St(t)*Pd(t) \qquad (21)$$

（但し’＊’は畳み込み演算を示す）

で表すことができ、さらに送信信号Ｓｔは基準信号であることから

$$Ds(t)=\Sigma((St(t+n)*Pd(t+n))\cdot R(-n))$$

$$=(R(t)*Pd(t))*R(t)$$

$$=R(t)*Pd(t)*R(t) \qquad (22)$$

となる。ここで

$$AR(t)=R(t)*R(t) \qquad (23)$$

を用いると（数２２）は

$$Ds(t)=AR(t)*Pd(t) \qquad (24)$$

となることがわかる。

一例として、基準信号に最長線形符号系列（Ｍ系列）を用いることを考える。Ｍ系列の符号は、（数２３）の自己相関関数ＡＲ（ｔ）が、ｔ＝０（０≦ｔ＜２＾ｎ－１）の場合２＾ｎ－１、その他では－１であるといった特長を有する（図２８（ａ））。このため、自己相関関数をインパルスと見なす事が可能で、周波数特性としてはこれを無視することが可能である。ある条件の下では、図６に示すような伝搬特性（遅延プロファイル）が求められるが、この周波数特性は則ち伝搬特性とシステム上のフィルタの特性との合成であることになる。一方、基準信号系列に合成符号の一種であるゴールド符号系列を用いた場合、Ｍ系列の符号とは異なり、自己相関関数ＡＲ（ｔ）のｔ≠０の部分において一定とはならない（図２８（ｂ））。このような自己相関関数はインパルスではなく、周波数特性として遅延プロファイルＤｓ（ｔ）に影響を与えてしまう。図２９に、基準信号をゴールド符号に置き換えた場合の推定結果を示すが、自己相関関数の影響を受け、図６とは波形が異なっていることが分かる。

この様に、（数２０）で示された通り、ここで求めた遅延プロファイルには、

基準信号系列の自己相関関数が含まれているため、基準信号系列の特性に影響されてしまうことがわかる。成分除去部２７０２は自己相関部２７０１が算出した自己相関関数（ＡＲ（ｔ））の成分を一次遅延プロファイルから除去する演算を行う。具体的には、自己相関関数で与えられるインパルス列をＩＩＲフィルタのタップ係数とすることで除去できることが知られている。

さらに、平均化演算部２７０３において、複数回演算した結果（２次遅延プロファイル）の平均化を施すことによって、歪やノイズにより発生する誤差を抑えることが可能となる。

このように、本実施の形態１４の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、等化部２６０２は、セキュリティデータを等化処理した後に復調するので、品質の良いセキュリティデータを得ることができる。また、本実施の形態１４の通信装置及び通信システムによれば、成分除去部２７０２は、基準信号の周波数成分を除去するので、基準信号の周波数成分の影響を受けない精度の良い伝搬環境の推定値を得ることができる。

なお、本実施の形態１４において、図２６に示す伝搬推定部１０３と図２６に示す受信復調部２６０４はそれぞれ独立して受信装置に組み込むことが可能であり、他の実施の形態で示した装置に適用可能であることは明白である。特に、これらを一緒に実施することでより大きな効果が期待できるといった特長を有する。

（実施の形態１５）

図３０は、本実施の形態１５の通信装置に係る伝搬推定部１０３の構成を示した図である。なお、伝搬推定部１０３を適用した通信装置は、図１と同一構成であるので、その説明は省略する。

バッファ３００１は遅延プロファイルを一時記憶し、ベクトル量子化部３００２は記憶された遅延プロファイルをコードブック３００８の内容と照合し最も類似したコードを出力し、符号変換部３００３はベクトル量子化されたコードを入力しこのコードと対応する符号をコードブック３００８の符号格納

部３００７から求め符号を出力し、自己相関部３００４は基準信号系列を入力しその自己相関関数を出力し、畳込演算部３００５はコードブック３００８のうち量子化ベクトルの内容に自己相関関数を畳み込むものであり、コードブック３００８はベクトル量子化の際に参照する量子化ベクトルとそれに対応する符号を格納し、図５に示すような構成でなる。コードブック３００８は量子化ベクトル格納部３００６とそれに対応する符号格納部３００７とからなっており、これらの構成は他の実施の形態と同一である。

次に、伝搬推定部１０３の動作について説明する。

受信信号がバッファ４０１により一時記憶され、この受信信号系列と基準信号系列格納部４０２が出力する基準信号系列とがコンボルバ４０３に入力される。コンボルバ４０３では、基準信号系列と受信信号系列とのスライディング相関演算を行うことで、遅延プロファイルを求める。これら遅延プロファイルはバッファ４０１により一時保存され、ベクトル量子化部３００２に送られる。一方、基準信号系列格納部４０２から出力された基準信号系列は、自己相関部３００４によって自己相関が演算されその値が畳込演算部３００５へと送出される。ベクトル量子化部３００２は、入力された遅延プロファイルとコードブック３００８にある量子化ベクトル格納部３００６の各ベクトルとのメトリクス量を演算し、その値が最小になるようなベクトルを選択するが、その際、自己相関部３００４によって自己相関関数が畳み込まれたベクトルを用いてメトリクス演算を行う。ベクトル量子化部３００２はこのようにして選択したベクトルコードを出力する。符号変換部３００３は、ベクトル量子化部３００２が出力したベクトルコードと、コードブック３００８にある符号格納部３００７から対応する符号を選択し伝搬推定情報を出力する。

このように、本実施の形態１５の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、畳込演算部３００５は、ベクトル量子化の際に量子化ベクトルに自己相関関数を畳み込むので、高精度なインパルス応答特性を得ることができる。また、本実施の形態１５の通信装置及び通信システムに

よれば、伝搬推定情報を高精度に求めるといった効果を有する。また、本実施の形態１５の通信装置及び通信システムによれば、量子化ベクトル格納部３００６にあるベクトルに基準信号系列の自己相関関数を畳み込むことで、探索するベクトルに自己相関関数ＡＲ（ｎ）の成分を与えることと等価となり、（数２０）で与えられるＤｓ（ｔ）にあるＡＲ（ｎ）に左右されずに探索する事が可能となり、基準信号系列の自己相関関数に左右されない量子化ベクトルの設定が可能となる。また、本実施の形態１１の通信装置及び通信システムによれば、自己相関関数を量子化ベクトルに自己相関関数の成分を加えるため、畳込演算を行うのみで可能であり、容易に実現が可能になるといった大きな特長を有する。

（実施の形態１６）

図３１は、本実施の形態１６に係る受信装置３１００の構成を示す図であり、図３２は、伝搬推定部１０３、変換部３１０１及び符号化部１０５の構成を示す図である。なお、図１と同一構成の部分には同一の符号を付してその説明は省略する。

変換部３１０１は、遅延プロファイルをフーリエ変換し、フーリエ変換した係数の中で主要な係数を選択して出力する。

次に、伝搬推定部１０３、変換部３１０１及び符号化部１０５の構成について、図３２を用いて説明する。図３２は、フーリエ変換手段を加えることで効率的な符号化を可能にする方法について示したものである。

最初に、伝搬推定部１０３について説明する。

バッファ３２０１は、入力した受信信号を一定長だけ一時保持する。

基準信号系列格納部３２０２は、予め定められた基準信号系列を格納、順次出力する。

コンボルバ３２０３は、一時保持された受信信号と基準信号系列を畳み込み演算して相関値を出力する。

バッファ３２０４は、算出された相関系列を一時保持する。

次に、変換部３１０１について説明する。

フーリエ変換部３２０５は、遅延プロファイルを入力しそれをフーリエ変換等の直交変換する。

係数抽出部３２０６は、フーリエ変換した係数を入力し主要な係数のみを選択する。

次に、符号化部１０５について説明する。

ベクトル量子化部３２０７は、コードブック３２０９に記録された量子化ベクトルの中から、入力されたベクトル列に最も類似したものを検索しコードを出力する。

符号変換部３２０８は、ベクトル量子化部３２０７が出力するコードに対応する暗号鍵をコードブック３２０９から選択し、出力する。

コードブック３２０９は、図５に示すように、量子化ベクトルと暗号鍵が格納されている。

図３３は、具体的な遅延プロファイルの状態を示したものであり、横軸は時間（図ではサンプルタイミング）、縦軸は信号振幅で示されている。相関値は、受信信号系列の同相成分（Ｉ成分）と直交成分（Ｑ成分）の夫々から求めており、図中の実線はＩ成分の相関係数、破線はＱ成分を示している。以下、Ｉ成分およびＱ成分は複素数の実数部および虚数部として表すこととする。また、一定時間内における最大の瞬時振幅を有する複素信号により正規化してある。

図３３に、基準信号系列が生成され、遅延プロファイルが得られるまでのブロックダイアグラムを示す。図３３に示されるとおり、送信装置２００では、基準信号系列格納部３３０１で生成された基準信号系列が、まず帯域制限フィルタ３３０２によって出力信号の波形形成が為される。この信号は、送信部３３０３によって空間に放射される。放射された電磁波は、様々な反射、回折などで形成される伝搬空間３３０４を通じて受信装置１００へと到達する。受信装置１００では、まず受信部３３０５で受信された受信信号系列は、帯域制限フィルタ３３０６によって、帯域制限されチャネル選択やノイズ成分除去が為

される。受信信号は帯域制限された後、相関部３３０８で基準信号系列格納部３３０７が出力する基準信号系列との相関を求め、送信装置２００が出力した基準信号系列を抽出する。以上の事について、数式を用いて説明する。（数１７）で与えられる受信信号Ｓｒ（ｔ）には、帯域制限フィルタ３３０６（Ｆｒ（ｔ））が施されている事から、

$$Sr'(t) = Fr(t) * Sr(t)$$
$$= Fr(t) * (St(t) * Pd(t)) \quad (25)$$

となる。式２５の送信信号Ｓｔ（ｔ）は基準信号系列に帯域制限フィルタ３００２（Ｆｔ（ｔ））を通過していることから、

$$Sr'(t) = Fr(t) * ((Ft(t) * Rs(t)) * Pd(t)) \quad (26)$$

である。遅延プロファイルを求めるには、前述の通り基準信号系列Ｒｓ（ｔ）との相関系列を畳み込み演算することで得られるから、

$$Ds(t) = Sr'(t) * Rs(t)$$
$$= Fr(t) * Ft(t) * Rs(t) * Rs(t) * Pd(t)$$
$$= F(t) * ARs(t) * Pd(t) \quad (27)$$

で与えられることになる。この時、Ｆ（ｔ）を帯域制限フィルタ３３０２と帯域制限フィルタ３３０６との合成特性で示されるインパルス応答であり、このフィルタ特性を帯域制限フィルタと呼ぶことにする。一方、ＡＲｓ（ｔ）は基準信号系列Ｒｓ（ｔ）の自己相関関数を示している。この様にして求められた（式２７）は自己相関関数ＡＲｓ（ｔ）に伝搬特性Ｐｄ（ｔ）を重畳した信号が、帯域制限フィルタによって帯域制限された特性を表している。ここで自己相関関数ＡＲｓ（ｔ）がインパルス特性であるとすると、伝搬特性Ｐｄ（ｔ）に帯域制限フィルタが掛かった特性と等価であることになる。

伝搬特性Ｐｄ（ｔ）を周波数特性として考えた場合、Ｆ（ｔ）によって与えられる周波数特性を加えた伝搬特性がＤｓ（ｔ）として求められる事がわかる。例えば、Ｆ（ｔ）が－１／２ｆｂｗ～＋１／２ｆｂｗの帯域制限フィルタであ

るとした場合、ｆｂｗで帯域制限された伝搬特性Ｐｄ－ｂｗ（ｔ）が求められる。室内伝搬などの環境では、伝搬特性の周波数特性は１ＭＨｚ以上の帯域が主要であることから、シンボルレートが１ＭＨｚ以上の通信に於いて特に有効であることがわかる。一方、屋外伝搬の場合は、伝搬特性の周波数特性は１０ｋＨｚ以上の帯域が主要であることから、シンボルレートが１０ｋＨｚ以上の通信に於いて有効である。

さて、受信信号から求めた伝搬特性Ｄｓ（ｔ）には、Ｆ（ｔ）で与えられる周波数帯域に制限された伝搬特性成分のみが求まるため、Ｄｓ（ｔ）を変換部３１０１のフーリエ変換部３２０５によって周波数ドメイン領域に変換することで、パラメータが低域部分に集中する事がわかる。このようにして周波数ドメイン領域に変換した信号系列の内、周波数の低域部分のみを選択・抽出する係数抽出部３２０６によって、伝搬特性の主要な成分を少ないパラメータで表現することが可能となる。具体的には、図２９に伝搬特性として求められたＤｓ（ｔ）の波形を示す。この波形をフーリエ変換した信号系列を図３４に示す。図３４を見ると分かるとおり、約１２の要素に主要な信号成分が凝縮されていることが分かる。これは、換言すると図２９で示した１００サンプル×２要素以上の信号系列がおよそ１０程度の要素で表現が可能であることを示しており、このことから非常に簡易な構成でベクトル量子化が可能になることを意味する。

このように、本実施の形態１６の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、変換部３１０１は、伝搬推定値をフーリエ変換して主要な係数のみを抽出するので、伝搬環境を最も如実に数値化することができる。また、本実施の形態１６の通信装置及び通信システムによれば、ベクトル量子化部３２０７は、変換部３１０１にて伝搬推定値をフーリエ変換して主要な係数のみを抽出した後にベクトル量子化するので、非常に簡易な構成でベクトル量子化が可能になる。また、本実施の形態１６の通信装置及び通信システムによれば、フーリエ変換して主要な係数のみを選択して符号化するので、

少ない伝搬パラメータで効率よく第１データを取得することができる。また、本実施の形態１６の通信装置及び通信システムによれば、変換部３１０１を伝搬推定部１０３と符号化部１０５との間に挿入することで、大幅な簡略化が可能になるといった非常に大きな特長を有する。

なお、本実施の形態１６においては、変換部３１０１にてフーリエ変換を用いた、これに限らず、他にもＤＣＴ（離散コサイン変換）や、ウェーブレット変換、ヒルベルト変換などに置き換えても同様の効果が得られることが知られている。

（実施の形態１７）

図３５は、本実施の形態１７に係る送信装置３５００の構成を示す図であり、図３６は、本実施の形態１７に係る受信装置３６００の構成を示す図である。送信装置３５００は、送信データを変調信号に加えて、受信端での信号電力に重畳して通信を行う。受信装置３６００は、受信信号の受信電力から重畳された情報を検出する。

最初に、送信装置３５００について説明する。

変調部３５０１は第１送信データを一時保持しチャネル数分のチャネル変調信号を出力し、拡散符号格納部３５０２はチャネル数分の拡散符号を格納しそれを出力し、拡散部３５０３はチャネルデータとチャネルに対応する拡散符号を畳み込み演算し周波数拡散を行い、伝搬制御部３５０４は第１送信データを入力しチャネル毎にアンテナ係数を算出し、合成部３５０５は拡散信号にアンテナ係数を乗じ信号合成したアンテナ信号を出力し、送信部３５０６は重み付け信号を周波数変換し増幅し、アンテナ部３５０７は対応する系列の信号を放射する。

次に、受信装置３６００について説明する。

アンテナ部３６０１は受信ＲＦ信号を出力し、受信部３６０２は受信ＲＦ信号を入力し電力増幅や周波数変換を行い、拡散符号格納部３６０３はチャネル数分の拡散符号を格納しそれを出力し、逆拡散部３６０４はチャネルに対応す

る拡散符号と受信信号とを畳み込み演算により逆拡散しチャネル信号を出力し、復調部３６０５はチャネル信号を夫々入力して復調しチャネル復調信号を出力し、電力検出部３６０６はチャネル毎の受信電力を検出し受信電力情報を出力し、バッファ３６０７はチャネル復調信号を一時保持し第２データを出力し、比較部３６０８は受信電力情報を入力しその大きさを比較して第１データを出力する。

次に、送信装置３５００及び受信装置３６００の動作について、図３７を用いて説明する。図３７は、伝搬情報として得られる受信電力に情報を重畳する通信方法について説明したものである。

図３７では、送信装置を図３５と同一構成とするとともに受信装置を図３６と同一構成にするものであるが、便宜上このように説明するだけで両装置ともに送受信可能な端末であってもよい。

（０）初期化

送信装置および受信装置は電源投入後、所定の初期動作を行い各種パラメータなどの値を所定の値に設定する。

（１）基準信号送信

受信装置は、伝搬状態を検出するための基準信号を出力する。送信装置は、基準信号を検出するとその信号を基に受信装置からの伝搬状態を算出する。

（２）暗号送信

送信装置は、（１）で得られた伝搬状態を用いて、受信端における電力制御に情報を重畳して通信信号を出力する。受信装置は、通信信号を受信した受信信号を復調すると同時に、信号の受信電力を検出しこれに重畳された情報を検波する。以下、同様に手続きを行う。

次に、図３７の手続きに従って、各部位の動作を詳細に説明する。

ここでは、チャネルの数を３（チャネルＡ、チャネルＢ、チャネルＣ）、アンテナの数を４（アンテナ１、アンテナ２、アンテナ３、アンテナ４）とする。また、送信装置では、前述の通信手順（１）によって受信装置からの伝搬状態

が算出されているものとする。

第１データと第２データを入力すると、変調部３５０１は第２データを一時保持し、３チャネル数分のチャネル変調信号を出力する。チャネル変調信号は、拡散部３５０３へと送出され、拡散符号格納部３５０２から与えられる拡散符号との畳み込み演算により周波数拡散が行われ、チャネル拡散信号が出力される。伝搬制御部３５０４は、通信手順（１）によって得られた伝搬状態と、入力された第１データとを用いて受信端での電力が所定の状態になるようなアンテナ係数を出力する。

電力に情報を重畳する方法としては、各チャネルの電力の順番に重畳する方法や、チャネル間の電力の差や電力の比に情報を重畳する方法が考えられる。ここでは、電力の順番に情報を重畳する方法について述べる。

例えば、第１データを３チャネルの電力の順番に重畳する場合

チャネルＡの電力＞チャネルＢの電力＞チャネルＣの電力

チャネルＡの電力＞チャネルＣの電力＞チャネルＢの電力

チャネルＢの電力＞チャネルＡの電力＞チャネルＣの電力

チャネルＢの電力＞チャネルＣの電力＞チャネルＡの電力

チャネルＣの電力＞チャネルＡの電力＞チャネルＢの電力

チャネルＣの電力＞チャネルＢの電力＞チャネルＡの電力

といった具合に６通りの情報を重畳できる。

この６通りのパターンに夫々符号を割り当て、予め送信装置と受信装置で共有しておくものとする。

伝搬制御部３５０４は、第１データに対応する電力情報に応じて、チャネル変調信号に対するアンテナ係数を求める。

アンテナ係数を用いて電力を制御する方法について、図３８を用いて詳細に説明する。図３８では、送信装置と受信装置に設けられたアンテナと、送受アンテナ間で決定される伝搬係数および、各アンテナから入出力される信号との関係を表したものである。ここで、Ａ１～４は送信装置に設けられたアンテナ、

Ａｒは受信装置に設けられたアンテナ、Ｓｔ１～４は送信ＲＦ信号、Ｓｒｘは受信ＲＦ信号、ｈ１～４は伝搬係数である。また、図中に示した合成部３５０５は、図３５における合成部３５０５に相当するものであり、チャネル拡散信号Ｓｃ１～４とアンテナ係数Ｃ１１～Ｃ３４との演算関係を示している。（送信部は省略してある）これらの関係を数式に表すと

$$Srx(t) = \Sigma Stn \cdot hn$$
$$= \Sigma (\Sigma Scm \cdot Cmn) \cdot hn \qquad (28)$$

で与えられる。送信装置は、通信手順（１）の基準信号によって求めたｈ１～４の値から、Ｃ１１～Ｃ３４の値を調整することによりアンテナＡｒで受信される受信信号Ｓｒｘにおける受信電力をチャネル拡散信号Ｓｃ１～３について独立に調整可能である。特に、Ｃ１１～Ｃ３４の位相を変化させるだけで制御を行った場合、各アンテナから放射される電力が変化することがないといった特徴がある。

例えばチャネルＡ（Ｓｃ１）は、Ａ１～４から放射された信号が空間合成によってＡｒにおいて最大電力になるようにＣ１１～Ｃ１４が算出され、チャネルＢ（Ｓｃ２）は同様にしてノッチが形成されるようにＣ２１～Ｃ２４が算出され、チャネルＣ（Ｓｃ３）に関してはチャネルＡとチャネルＣとの中間の電力になるようにアンテナ係数Ｃ３１～Ｃ３４を算出する。

合成部３５０５では、アンテナ係数とチャネル変調信号とを入力し、アンテナ１～４に対するアンテナ信号が合成される。アンテナ信号は、送信部３５０６で周波数変換され電力増幅された後、アンテナ部３５０７で放射される。

この様にして出力された暗号化信号は、受信装置のアンテナ部３６０１で受信され、その受信ＲＦ信号が受信部３６０２へと送出される。受信部３６０２では受信ＲＦ信号を入力し、それを電力増幅、周波数変換した受信信号を出力する。受信信号は逆拡散部３６０４に入力され、拡散符号格納部３６０３から入力される拡散符号との畳み込み演算が行われる。逆拡散はチャネル数分（ここでは３チャネル分）に対して行われ、チャネル毎に分離されたチャネル信号

が出力される。復調部３６０５では、チャネル信号を入力しそれを復調してチャネル復調信号を出力すると共に、電力検出用にチャネル検出信号を出力する。バッファ３６０７では、復調部３６０５から入力したチャネル復調信号を一時保持し、第１データとして出力する。電力検出部３６０６はチャネル検出信号を入力し、チャネル毎の受信電力を推定し、チャネル電力情報を出力する。比較部３６０８では、チャネル電力情報で与えられる電力値を比較し、その結果から予めチャネル電力の順番に割り当てられた符号に変換し第１データとして出力する。

送信装置３５００が発した第１データは受信装置３６００で第１データとして用いることが可能となり、特に第２データは、送信装置３５００と受信装置３６００の間で形成される伝搬路を積極的に利用した通信であるため、他の受信装置では受信が出来ないといった特徴を有しており、セキュリティが重要な情報に対して有効な通信手段となることはいうまでもない。

以上の説明に加え、従来技術との差異について図３９～４２を用いて詳細に行う。図３９は従来技術としての例である。信号Ｓｃ１～３の出力電力をＣ１～Ｃ３により制御し、且つＷ１～Ｗ４を用いて指向性制御を行う例を示している。図３９と図３８では、図３９が全てのアンテナに対して同一の重み係数（Ｃ１～Ｃ３）を乗じている一方、図３８ではＳｃ１～３に対してアンテナ毎に重み係数（Ｃ１１～Ｃ３４）を独立して制御するような構成となっている。図３９の様に全アンテナに対して同一の重み係数を用いた場合、指向性で与えられた放射特性に対してその大きさの特性が与えられることになる。

図４０～４２は、空間の断面の位置を横軸に、その場所に於ける受信電力を縦軸にして、各信号の電力分布を描いたものであり▲印が、ターゲットとする受信端末の設置場所を示している。図４０は、図３９で得られる特性を示してある。図４０に示すとおり、全ての信号分布は相似形になっており、分布形状がＷ１～Ｗ４で与えられる指向性制御の特性を表している。このため、受信位置がターゲットとする位置からずれていても、受信信号電力は相対的に変化し

ない事がわかる。一方、図３８によって伝搬制御された信号分布を図４１に示す。送信信号は、各アンテナに対して異なる係数の組合せを有するため、（結果として指向特性が異なるため）受信位置によって各信号の受信電力が異なるといった特徴がある。則ち、ターゲットとする受信位置に対しては、制御したとおりの電力比となっている（●印）が、場所が異なると受信電力の比は異なってしまう。この事を利用することで、送信端末がターゲットとする受信位置以外では、受信電力を用いた復調は出来ないことになる。

また、図３８の重み係数Ｃ１１～Ｃ３４によって、受信電力が０となるヌル点の制御も可能である。このヌル点は出力アンテナの数をｎとするとｎ－１個のヌル点を制御することが可能であることが知られている。ここで、送信信号（例えばＳｃ１）を指向性制御によって、受信位置において十分な受信電力になるように制御し、一方、その他の送信信号（例えばＳｃ１、Ｓｃ２）を制御可能なヌル点の幾つか（或いは全て）をターゲットとする受信位置になるように制御する。このように、ｎ（ｎ≧２）個のアンテナからｍ種類（ｍ≧２）以上の信号を伝搬制御して送信し、その信号の伝送制御は受信アンテナに対して適切な電力が供給されるように制御し、一方、伝送する必要のない信号に対して送信制御は受信アンテナに対して最大ｎ－１のヌル制御を行うことが可能である。なお、ｍ種類の信号において、少なくとも１つが伝送するための信号であれば、伝送するための信号の数は２以上であっても良い。図４２にこの様に制御された状態を示す。

図４２では、破線で示された各信号（Ｓｃ２、Ｓｃ３）が▲の場所に於いてヌルを形成し、受信電力が低く制御されている一方、実線で示された信号（Ｓｃ１）は十分な受信電力が得られている様子が示されている。ここで送信端末は、Ｓｃ１に送信すべき情報を、Ｓｃ２、Ｓｃ３には疑似情報（或いは重要でない情報）を重畳しておくものとする。この様な通信を行うことで、ターゲットとする受信位置における受信信号は、Ｓｃ１のみとなるため、受信端末は受信信号をそのまま復調することでＳＣ１の情報を得ることが可能となる。一方、

その他の場所でこれらの信号を受信しようとすると、受信信号はＳｃ１～３の電力が入っているため、分離することが困難となる。また、仮に分離が可能であったとしてもＳｃ１～Ｓｃ３のどれが受信すべき情報であるかを推定不可能であるため、正しく復調することが出来ない。

この様にヌル点を制御する方法を用いると、受信時においてそもそも受信すべき情報しか受信しないため、受信端末は従来と同様の構成で構わない。則ち、送信端末のみを変更することでセキュリティが確保された通信を実施することが可能となるといった大きな特長を有する。

このように、本実施の形態１７の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、送信側の合成部３５０５は、複数のアンテナを用いて異なる伝搬路にて通信相手へ第１データを送信し、受信側の比較部３６０８は、異なる伝搬路を経由してきた到来波を受信して各経路の伝搬環境の推定値の比較結果より第１データを得るので、第三者の通信装置を用いて第１データを傍受することを極めて困難にすることができて高いセキュリティを確保することができる。また、本実施の形態１７の通信装置及び通信システムによれば、送信装置３５００は複数チャネルを周波数拡散したあと、これを多重する際にアンテナ係数を乗じてチャネル毎に伝搬状態を制御することで、伝搬状態（ここでは信号電力、則ち伝搬ロス）に情報を重畳することが可能となる。また、本実施の形態１７の通信装置及び通信システムによれば、信号電力に情報を重畳する手法としてＡＳＫに代表される振幅変調があるが、伝搬状態を積極的に利用する点、つまり受信アンテナ端における信号電力を用いているため他の受信点では伝搬特性が異なるために正常に受信できない点で大きく異なっている。たとえば、前述の通りアンテナからの出力電力を変化させることなく受信端における信号電力を変化させることが可能なため、第３者が送受信の通信を傍受し、これを復調しようとしても第２受信データを復調することは不可能であることから高いセキュリティを確保できるといった大きな特長を有する。また、本実施の形態１７の通信装置及び通信システムによれば、マルチ

キャリア信号を用いキャリア間の信号電力差に着目して通信を行う様にすることで、同時に受信した信号から検波が行えるといった大きな特長がある。これは、同一時刻、同一周波数であることから、伝搬条件は同一のものであると見なせるため、安定した通信を提供することが可能になる。例えば、２チャネルを多重した拡散信号を用いる場合（チャネルＲとチャネルＳとする）、チャネルＲを基準として、その信号電力に対してチャネルＳの信号電力が大きいか小さいかを符号に割り当てることも考えられる。信号位相に情報を多重する場合は、同様にしてチャネルＲの基準位相に対してチャネルＳの基準位相を検出したりする事も考えられる。

なお、本実施の形態１７において、周波数拡散通信を例に説明を行ったが、これに限らず、ＯＦＤＭなどのマルチキャリア信号にも適用可能であるし、シングルキャリア信号でも可能である。ＯＦＤＭ通信においては、拡散、逆拡散がＩＦＦＴ、ＦＦＴに置き換え、チャネルをサブキャリアに置き換えることで容易に実現が可能である。ＯＦＤＭの場合、伝搬特性がサブキャリアの電力に現れるので、この包絡線をパラメータとして符号を割り当てるなどすればよい。

また、本実施の形態１７において、伝搬を通じて合成された信号電力に情報を重畳する方式に付いて説明を行ったが、これに限らず、当然信号の位相や周波数などにも重畳することは可能であり、さらに偏波や遅延プロファイルなどに情報を重畳することが可能であるといった特徴がある。

また、本実施の形態１７において、アンテナの構成として偏波面の異なる（例えば偏波面が直交する）アンテナを配することで、前述の通り偏波に信号を重畳することも可能である。この場合には、特にマルチキャリア信号である必要はないが、マルチキャリア信号を用いる場合、チャネルＲの偏波面を基準としてチャネルＳの偏波面の角度に情報を重畳するなどが考えられる。

また、本実施の形態１７において、遅延プロファイルに情報を重畳する場合、マルチキャリア信号を用いることで、チャネルＲから得られる遅延プロファイルを基準として、チャネルＳから得られる遅延プロファイルの差分に情報を重

畳することも考えられ、この様にすることで遅延プロファイルが対象とする伝搬状態の同一性が保たれるため、精度の高い通信が期待できるといった特長を有する。また、実施の形態１７において、同一時刻でかつ同一周波数に秘匿情報と疑似情報を重畳することによって、ターゲットとする受信位置でのみの通信を可能とし、秘匿性の高い通信方式を提供することができる。

（実施の形態１８）

本実施の形態１８は、上記実施の形態１７で説明した発明をさらに拡張して複数の受信信号系列から得られる夫々の伝搬パラメータに対して情報を重畳する点を特徴とするものである。

図４３は、本実施の形態１８に係る通信装置である受信装置４３００の構成を示す図であり、図４４は、本実施の形態１８に係る通信装置である送受信装置４４００の構成を示す図である。なお、図９及び図３６と同一構成である部分には同一の符号を付してその説明は省略する。

本発明の実施の形態１８に係る通信装置である受信装置４３００は、図３６に示す本発明の実施の形態１７に係る受信装置３６００において、受信部３６０２の代わりに受信部４３０２ａ、４３０２ｂを有し、逆拡散部３６０４の代わりに逆拡散部４３０３ａ、４３０３ｂを有し、復調部３６０５の代わりに復調部４３０４ａ、４３０４ｂを有している。

受信部４３０２ａ及び受信部４３０２ｂは、受信装置４３０２を構成している。逆拡散部４３０３ａ及び逆拡散部４３０３ｂは、逆拡散装置４３０３を構成している。復調部４３０４ａ及び復調部４３０４ｂは、復調装置４３０４を構成している。

受信部４３０２ａは、アンテナ４３０１ａから入力した受信ＲＦ信号を電力増幅及び周波数変換して逆拡散部４３０３ａへ出力する。

受信部４３０２ｂは、アンテナ４３０１ｂから入力した受信ＲＦ信号を電力増幅及び周波数変換して逆拡散部４３０３ｂへ出力する。

逆拡散部４３０３ａは、受信部４３０２ａから入力した受信信号とチャネル

に対応する拡散符号とを畳み込み演算により逆拡散してチャネル信号を復調部４３０４ａへ出力する。

逆拡散部４３０３ｂは、受信部４３０２ｂから入力した受信信号とチャネルに対応する拡散符号とを畳み込み演算により逆拡散してチャネル信号を復調部４３０４ｂへ出力する。

復調部４３０４ａは、逆拡散部４３０３ａから入力したチャネル信号を復調してチャネル復調信号を選択合成部４３０５へ出力するとともに、通信制御部４３０６の出力指示信号にしたがって復調信号を電力検出部３６０６へ出力する。

復調部４３０４ｂは、逆拡散部４３０３ｂから入力したチャネル信号を復調してチャネル復調信号を選択合成部４３０５へ出力するとともに、通信制御部４３０６の出力指示信号にしたがって復調信号を電力検出部３６０６へ出力する。

選択合成部４３０５は、通信制御部４３０６から入力した選択合成信号に基づき、各アンテナから受信したブランチ受信信号（或いはブランチ受信データ）を選択（或いは合成）した後、選択合成結果を第２データとして出力する。この様にすることで、伝搬空間を時刻によって切り換える効果が得られるため、空間ダイバーシチのような利得が得られる。

通信制御部４３０６は、定められた時間に定められたアンテナからのブランチ受信信号（或いはブランチ受信データ）を選択・合成するように選択合成信号を選択合成部４３０５へ出力する。また、通信制御部４３０６は、秘匿情報が含まれている信号を受信したアンテナ４３０１ａ、４３０１ｂの復調信号を電力検出部３６０６へ出力させるための出力指示信号を復調部４３０４ａ、４３０４ｂへ出力する。これにより、第３者からは伝搬空間を推定することが不可能なため、アンテナ４３０１ａ、４３０１ｂの通信信号を分離することが不可能であり、より高度なセキュリティを実現することが可能になると言った有利な特長がある。

比較部３６０８（伝搬パラメータ差算出手段）は、アンテナ素子４３０１ａにて受信した受信信号の受信電力とアンテナ素子４３０１ｂにて受信した受信信号の受信電力との差分（伝搬パラメータ差）を算出し、算出した差分情報を第１データとして出力する。

図４５は、送信装置と受信装置に設けられたアンテナと、送受アンテナ間で決定される伝搬係数および、各アンテナから入出力される信号との関係を表した図である。図４５は、図３８の受信アンテナ数を１本から２本に拡張したものである。

以上のように構成されたシステムにおいて、アンテナＡｒ１、Ａｒ２における受信信号は以下の式で与えられる。

$$Srx1(t) = \Sigma Stn \cdot h1n$$
$$= \Sigma(\Sigma Scm \cdot Cmn) \cdot h1n \quad (29)$$
$$Srx2(t) = \Sigma Stn \cdot h2n$$
$$= \Sigma(\Sigma Scm \cdot Cmn) \cdot h2n \quad (30)$$

式（２９）、式（３０）からも分かるとおり、Ｓｒｘ１とＳｒｘ２は伝搬路の構成が異なるため、伝搬パラメータｈ１ｎ、ｈ２ｎも異なってくる。これらＳｒｘ１とＳｒｘ２の受信状態は、式（２９）、式（３０）で示すＣｍｎの操作によって制御可能である。受信端末では、Ｓｒｘ１で得られる伝搬状態とＳｒｘ２で得られる伝搬状態とを比較した結果を情報として復調・復号に供することも考えられる。則ち送信側ではＳｒｘ１とＳｒｘ２で制御する伝搬パラメータの差分（位相差分や受信電力差などが考えられる）に対して情報を重畳させて送信し、一方受信側ではＳｒｘ１とＳｒｘ２の各受信信号から求めた伝搬パラメータの差分を算出し、この差分を通信情報の一部或いは全部とすることで通信する事により、より多様な通信を可能とする。さらにこの様にして通信を行うことで、２系統分の伝搬パラメータを推定する必要性が生じ、そのため高度なセキュリティを確保することが可能になる。当然、アンテナの数を増加させることでより高度なシステムを構築可能であり、こうすることでセキュリ

ティの向上が見込める。

また、複数のアンテナＡｒ１、Ａｒ２を用いてセキュリティ通信を行うことも可能である。アンテナＡｒ１とアンテナＡｒ２とは伝搬パラメータが異なるため、受信される信号が異なることは前述の通りである。このことを利用すると、アンテナＡｒ１に対する変調信号とアンテナＡｒ２に対する変調信号を夫々制御することで、アンテナＡｒ１に対してのみ秘匿情報を伝送したり、アンテナＡｒ２に対してのみ秘匿情報を伝送したり、或いは両アンテナＡｒ１、Ａｒ２に対して秘匿情報を伝送したり、これらの状態を定められた時間で切り換えたりする事で、より複雑で高度なセキュリティ通信を可能にする。

図７１を用いて具体的に説明する。図４２と同一の内容であるが、ターゲットとする場所が１箇所から２箇所に増えた場合を示している。図４２には上下にグラフが分割されて記載されているが、図４２と同様電波の電力分布を示したものである。上下のグラフは同一断面を表している。たとえば実施の形態１７で説明したように、２箇所にヌルを形成してこれを所定の時間で切り替えて出力した場合、上のグラフと下のグラフとが切り替わったようになるが、このようにして、受信機側でもそれに同期させて切り替えることによって実施の形態１７と同様に通信が可能になる。さらに、図７６に示すようにヌルを対応する２箇所に形成して通信を実施すると、不要成分が両アンテナに入らないため同様に通信が行えるようになる。さらに、アンテナＡｒ１、Ａｒ２でそれぞれ受信した信号は、伝搬係数を利用することで図中の太い実線と太い点線とを分離可能になる。受信アンテナの数がｎ（Ａｒ１・・Ａｒｎ）であれば、時空間多重（ＳＤＭ（Space Division Multiplex）やＭＩＭＯ（Multi-Input Multi-Output））することで、図４２に比べ通信容量をｎ倍に拡大することも可能である。当然、時空間符号化（Ｓｐａｃｅ－Ｔｉｍｅ　Ｃｏｄｅ）することで、特性の大幅な改善も見込まれる。このため、通信容量・通信品質の観点から非常に有利な特長をもつ。

さらに、このように通信を行った場合、図４５に示したようにチャネルを構

成するパラメータ要素が多くなるため、第３者へ情報が漏洩する危険性が大幅に減るといった大きな特長を有する。また、この秘匿通信をＭＩＭＯなどで利用されている空間分離用のパイロット信号や通信の位相・振幅の基準信号に対して実施しても同様の効果が得られる。

上記では、伝搬特性に応じてアンテナ係数（重み付け係数）を演算するとしたが、この計算方法について説明する。ここでは、ｎ行×ｍ列の行列Ｈを例に挙げる（則ち送信アンテナ数ｎ、受信アンテナ数ｍの場合となる）。全ての行列Ｈは直交行列Ｕ（ｍ行ｍ列）、Ｖ（ｎ行ｎ列）と特異値行列Ｓ（ｎ行ｍ列）を用いて、

$$U \times S \times V' = H \qquad (31)$$

ここでＶ’はＶのエルミート転置を意味している。

この様に分解された直交行列Ｕ（或いはＶ）はｍ×１（１×ｎ）の特異値ベクトルをｍ（ｎ）個並べた行列であると見なし、これをｕ１～ｍ（ｖ１～ｎ）とする。

この時、ｕ１～ｍ（ｖ１～ｎ）は、

$$ux \times H = \lambda x \qquad (\text{または} Hx \times vx = \lambda x) \qquad (32)$$

である。λｘはｕｘ（ｖｘ）に対応する特異値である。この時、伝搬特性を表す行列Ｈを特異値分解し、特異値λｘ＝０である固有ベクトルｕｘの各要素をアンテナ係数（重み付け係数）とすることで受信アンテナ端での受信電力を０に制御することが可能となる。

次に、図４４を用いてより詳細に説明する。図４４は、図９とほぼ同様の構成によって為されており、図４４においてはベクトル量子化を行わないため、図９の構成から符号化部１０５、コードブック９０５を除いたものとなっている。以下、図９との相違点のみについて説明する。伝搬推定部１０３は、受信した受信信号から端末間の伝搬特性（伝搬行列Ｈ）を算出する。この伝搬特性は係数算出部９０３へ送出され、係数算出部９０３で伝搬行列Ｈの特異値分解を行う。このうち、対応する特異値λｘ≠０である特異値ベクトルｖｘ（ｘ＝

1、・・・、p）、λx＝0である特異値ベクトルvx（p＋1、・・・、n）とする。ここでは便宜上前者を特異ベクトル、後者をゼロベクトルと呼ぶことにする。これらは全てバッファ９０４に一時保存される。一方、通信情報１～kが変調部９０６へと入力されそれぞれ対応する変調信号１～kが出力される。特異値ベクトルと変調信号はそれぞれ重み付け部９０７に入力され、秘匿化したい通信情報に対応する変調信号（ここで通信情報１、変調信号１とする）と特異ベクトル（ｖ１～ｖｐ）のうちどれか（例えば特異値の最大のもの、或いは幾つかまたは全てを加算したベクトル）をベクトル乗算する。更に秘匿性を高めたい場合、受信装置に対して不要な通信情報（ここで通信情報３、変調信号３とする）に対して、重み付け部９０７で乗ずる係数をバッファ９０４で保持された特異値ベクトルのうち、ゼロベクトル（ｖｐ＋１～ｖｎ）のうちどれか（幾つか或いは全てを加算したベクトル）をベクトル乗算する。これらベクトル演算された変調信号ベクトルは送信部９０８に入力される。送信部９０８は、各変調信号ベクトルは対応するアンテナの信号系列毎に加算された後に周波数変換され、アンテナ９０１を介して放射される。

この様にして放射された信号は伝搬空間を介して受信装置で受信されるが、伝搬空間の特性（伝搬行列Ｈ）と変調信号Ｓｍｏｄを用いて以下のように表される。

Ｈ×Ｓｍｏｄ×ｖｘ＝λｘ×Ｓｍｏｄ　　（３３）

数式３３からわかるように、特異値ベクトルが乗算されている変調信号１は受信装置に届くことが分かる。一方、変調信号３は特異値λｘ＝０であるベクトルが乗算されているため、受信装置には届かない。則ち、受信装置は受信信号をそのまま復調することで、変調信号１のみを復調することが可能になる。

以上のことは、即ち図４２、７１、７６に示したようなヌル制御を行っていることと等価である。つまり、ヌル制御によって秘匿通信を実施する場合は特異値分解を行い、これで得られる特異値ベクトルを活用することで容易に実施が可能であることを示している。

次に送受信装置でない第３の装置がこれらの信号を受信することを考えると、送信装置と共有する伝搬特性である伝搬行列Ｈ’が異なるため、数式３３は成り立たない。つまり、変調信号１、３は伝搬行列Ｈ’と先の特異値ベクトルとの相関により与えられ、この信号を変調信号１と３とに分解することは不可能である。

また、秘匿化しない通信情報に対応する変調信号（ここで通信情報２、変調信号２とする）に関しては、重み付け部９０７で乗ずる係数をバッファ９０４で保持された特異値ベクトル以外（或いは［１，１，・・・１］のような一定のベクトル）の係数を与えればよい。この場合、特異値ベクトルと異なる係数を与えているため、数式３３は成り立たず、受信装置に受信される。

以上説明したように、送信装置において、送信する変調信号を送信相手である端末との間で形成されている伝搬状態（あるいは伝搬パラメータ）によって分解し、分解した信号をそれぞれのアンテナから送信することで、受信端での信号は空間合成により元の変調信号になる。このとき、変調信号の分解方法としては、伝搬パラメータから導出される係数（数式３２の固有ベクトルの各要素に相当する値）をアンテナ係数（あるいは重み付け係数）として与え、元の変調信号とアンテナ係数との乗算によって行うことが可能である。この様にすることで、伝搬パラメータを共有できない第３の端末では空間合成の結果が異なるため、正しく復調できないという秘匿性を有する。

また、本通信方式の為に特別な構成を持たない受信装置であっても選択的な通信が行えることを示している。則ち、本発明は送信装置のみを変更することでセキュリティ通信を実現することが可能であると言った非常に大きな特長を有する。

このように、本実施の形態１８の通信装置及び通信システムによれば、上記実施の形態１及び実施の形態１７の効果に加えて、送信する変調信号を伝搬状態によって分解して各々の信号を異なるアンテナから送信するので、伝搬状態が異なる第３の端末では空間合成の結果が異なるために正しく復調できず、高

いセキュリティを確保することができる。また、本実施の形態１８において、同一時刻でかつ同一周波数に秘匿情報と疑似情報を重畳することによって、ターゲットとする受信位置でのみの通信を可能とし、秘匿性の高い通信方式を提供することができる。

なお、本実施の形態１８においては、アンテナＡｒ１、Ａｒ２が同一の端末に接続されていることを前提として説明したが、これに限らず、アンテナＡｒ１、Ａｒ２が夫々別の端末（例えば端末１と端末２）に接続されていても良い。こうすることで、端末１に対するセキュリティ通信と端末２に対するセキュリティ通信を同時に行うことも可能になり、効率の良いシステムを構築可能である。

（実施の形態１９）

本実施の形態１９は、受信信号に重畳されている伝搬特性を利用して端末特定を行う点を特徴とするものである。

図４６は、本実施の形態１９に係る受信装置４６００の構成を示す図である。なお、図１と同一構成である部分には同一の符号を付してその説明は省略する。

特徴抽出部４６０１とバッファ部４６０２は、伝搬特徴抽出部４６０６を構成している。特徴抽出部４６０１は、伝搬推定部１０３から入力した伝搬推定情報より伝搬状態の特徴を抽出して特徴抽出情報をバッファ４６０２及び端末判定部４６０３へ出力する。バッファ部４６０２は、記憶した伝搬状態に応じた特徴抽出情報をバッファ情報として端末判定部４６０３へ出力する。

バッファ部４６０４及び情報処理部４６０５は、信号処理選択部４６０７を構成している。

特徴抽出部４６０１は、受信信号から得られた伝搬情報を入力して符号化することによりその特徴を抽出する。特徴を抽出する要素としては、位相特性、ゲイン特性、偏波特性、伝搬遅延特性、遅延分散特性、到来方向推定による角度プロファイルなどが挙げられる。これらの要素を単独あるいは要素の組み合

わせて得られる特徴をアナログ値として標本化しても構わない。この場合、特に特徴抽出する必要はなく端末判定部４６０３での判定もアナログ情報での比較となるためより高度で精度の高い判定が可能となる。一方、特徴を抽出する方法としてフーリエ変換やディスクリートコサイン変換、ウェーブレット変換などに代表される変換や、フィルタやマルチバンドフィルタなどのフィルタ、或いは線形予測法に基づく係数抽出などが考えられる。また、特徴抽出部４６０１は、図１などで用いられている符号化部１０５と同一の構成とすることも可能である。図４で示すように符号化部１０５をベクトル量子化の手法を用いることで、多様な信号系列を１つの符号として表すことが可能となるため、端末判定を行う際の比較が容易になると言った特長がある。

バッファ部４６０６は、抽出した特徴抽出情報を一時的に記憶して、所定のタイミングにて記憶した特徴抽出情報をバッファ情報として端末判定部４６０３へ出力する。

端末判定部４６０３（判定手段）は、特徴抽出部４６０１から入力した特徴抽出情報とバッファ部４６０６から入力したバッファ情報を比較して一致具合を判定し、その判定結果を端末判定信号（第１データ）として情報処理部４６０５へ出力する。端末判定部４６０３は、一定時間で得られる伝搬情報を用いて最終的な端末判定結果を端末判定信号として２値信号で出力する。この場合、上述したように１／０のような２値信号ではなく０～９のような多値信号とすることでより柔軟なシステムを構成することも可能である。また、端末判定部４６０３は、特徴抽出部４６０１にて係数抽出する場合には、求められた係数列同士から両者のユークリッド距離を求め、その値が一定値以下であれば同一の端末であると判定し、そうでなければ異なる端末と判定する。判定の際、ノイズや伝搬特性の揺らぎなどにより判定結果が安定しない場合、一定の間判定結果を保存しておき一定時間の平均を取った後に判定する方法などが考えられる。そのような場合、判定結果を同一か異なるかを表す０／１の２値とするのではなく確からしさの値として０～９の様に幅を持たせることも考えら

れる。特に、端末判定を厳格に行おうとすると、結果に誤判定が出やすくなるため確からしさの値を一定期間で求められる平均値を元に判定を行うなどする事でより安定した端末判定が行える。このように、端末判定部４６０３は、推定した伝搬環境に基づいて現在通信している端末を監視し、悪意により通信している端末が知らぬ間に入れ替わってしまうこと等により秘匿情報が漏洩してしまうことがないように監視している。

バッファ部４６０４は、復調部１０４より入力した受信データを一定期間記憶する。

情報処理部４６０５は、バッファ部４６０４に記憶されて入力した受信データ列と端末判定部４６０３から入力した端末判定結果とから情報処理の内容を切り換えて変更する。例えば、受信したデータのうち、端末に大きく依存するようなプライバシ情報や課金情報、秘匿情報などはその処理を行わずにエラー処理として受信データを全て破棄することが考えられる。他に、端末判定結果により違う端末からのアクセスであると判断された事を伝送し、セキュリティ対策処理を行うなどの方法が考えられる。

次に、受信装置４６００の動作について説明する。

ここでは、端末特定を行う通信端末を通信端末１、その通信相手を通信端末２として説明を行う。ここで、通信端末２が出力した信号に対して、端末登録・端末判定の動作を行うため、説明では端末２が出力する場合のみについて説明する。

第１に、通信端末１は通信端末２の端末登録動作を行う。

通信端末１は通信端末２からの基準信号をアンテナ１０１で受信し、そのＲＦ信号が受信部１０２に入力され受信信号が出力される。受信信号は伝搬推定部１０３に入力され受信信号と基準信号とから伝搬特性を推定し伝搬情報を出力する。出力された伝搬情報は伝搬特徴抽出部４６０６へ入力され、特徴抽出部４６０１でその特徴抽出情報が出力される。この特徴抽出情報は、通信相手である通信端末２を特定する情報としてバッファ部４６０６に記憶される。

以上で、端末登録動作は完了する。

第２に、通信端末１は通信端末Ｘとの間で情報の授受を行うと共に、通信端末Ｘが登録された端末（通信端末２）であることの判定を行う。

通信端末１は通信端末Ｘからの通信信号をアンテナ１０１で受信し、そのＲＦ信号が受信部１０２に入力され受信信号が出力される。受信信号は伝搬推定部１０３に入力され受信信号から伝搬特性を推定し伝搬情報を出力する。伝搬情報は特徴抽出部４６０１、受信部１０２及び復調部１０４へ出力される。受信部１０２では伝搬情報に基づいて周波数補正、時間補正、ゲイン補正などを行いながらＲＦ信号から受信信号へ最適な状態を保つように制御される。復調部１０４は、受信信号を入力し、伝搬情報を元に周波数・位相補正、時間補正、ゲイン補正などを行いながら検波・復調し、受信データ系列を出力する。

次に、端末判定を行う場合の通信手順について、図４７を用いて説明する。以下、端末特定を行う側を基地局（図４７中では受信装置）、端末特定される側を端末（図４７中では送信装置）として説明する。

（０）基地局、端末：初期化

基地局、端末共に、電源が投入された直後、或いは特定の信号を受けて初期状態にセットされる。同時に、周波数や時間同期などの状態は事前に定められた手順に従ってセットされる。

以上のこれらの初期動作が終了した一定時間後、受信装置は一定時間毎に制御情報を制御信号に載せて送信する。

一方、基地局は初期動作が終了した後、制御信号のサーチを始める。端末が基地局から送信した制御信号を受信すると、その時刻、周波数などを検出してシステムが保有する時刻・周波数に同期する（システム同期）。システム同期が正常に終了した後、端末はその存在を基地局に通知するために登録要求信号を送信する。基地局は、端末からの登録要求に対して、登録許可信号を送信することで端末の登録許可を行う。

（１）端末：基準信号送信

端末は、基地局で行う伝搬推定用の基準信号を基準信号として出力する。具体的動作は、第１の実施の形態などで示した方法と同様の動作を行うが、基地局がこの通信で求めた伝搬情報からその特徴を抽出し、端末特定のための情報として求められた伝搬特性の特徴情報を該当する端末情報と共に登録する。

（２）基地局：通信信号送信

基地局は、通信を開始し通信信号を出力する。暗号化通信を行う場合は他の実施の形態で述べた方法などを用いて暗号化信号を出力しても良い。

端末は、通信信号を受信すると受信復調部１５０が受信信号を復調情報へと復調し、復調データを出力する。通信に暗号化が行われていた場合、他の実施の形態で述べた方法などを用いて復号する。

（３）端末：通信信号送信

端末は、通信信号を送信する。基地局は、受信部１０２からの受信信号から伝搬特性を推定し、その伝搬情報から特長情報を抽出する。同時に受信信号の復調を行い、受信データを出力する。この特徴情報と（１）で登録した特徴情報とを比較し、端末の判定を行う。こうして得られた判定をまとめた最終判定結果の可・否情報と受信したデータを出力する。信号処理選択部４６０７では、受信データと端末判定信号を入力しそのうち受信データを一定期間バッファ部４６０４に記憶する。一方、端末判定部４６０３は一定時間で得られる伝搬情報を用いて最終的な端末判定結果を端末判定信号として２値信号で出力する。情報処理部４６０５では、バッファ部４６０４に記憶された受信データ列と端末判定結果とから情報処理の内容を切り換える。例えば、受信したデータのうち、端末に大きく依存するようなプライバシ情報や課金情報、秘匿情報などはその処理を行わずにエラー処理として受信データを全て破棄することが考えられる。他に、端末判定結果により違う端末からのアクセスであると判断された事を伝送し、セキュリティ対策処理を行うなどの方法が考えられる。

以下、（２）（３）の暗号通信や通常の通信を繰り返す。

以上の手順に基づいて通信を行うことで、受信信号とそれを出力した端末と

の照合が可能になる。特に端末判定を行う本方式については（２）の手順は必要ではなく、（１）および（３）の手順のみで実施することが可能である。

また、（３）の操作に於いて判定結果に基づいてその後の情報処理動作を変えて実施することも考えられる。このように判定結果に基づいて処理を切り換えることにより、より処理の安全性を保つことが出来ると共に、正常に認証できない端末によるデータ詐称などを防ぐことが可能となるため、非常に高いセキュリティを持った装置やシステムが構築できると言った特長を有することが出来る。

通信端末間に形成される伝搬路の特性は、端末の位置や周囲のレイアウトなどで定まり、これを任意の特性に変更することは不可能である。複数のアンテナを用いて伝搬を制御する方法も考えられるが、伝搬路特性は第３の端末からは測定が不可能であり予測することも困難であるため、これを操作して通信端末を詐称することは極めて困難であることが分かる。そのため、本発明を用いた端末特定方法は、非常に簡単に高い精度で実現することが可能である。

さらに、アンテナ１０１と受信部１０２を複数用いて２つ以上の受信信号系列から、２つ以上の伝搬路の特性を導き出すことで判定する端末との伝搬情報が多様化するため、より高精度な判定を行うことが可能となる。

上記の方法によると、判定結果に誤判定が出た場合に通信の大幅なロスとなってしまう可能性がある。これを緩和して安定した通信を確保するためには、端末判定で否の判断が為された場合、再確認を行うことも考えられる。この手順について図４７を用いて説明する。

（３’）端末：通信信号送信

基地局は、端末が出力した通信信号から得られる伝搬情報を利用して端末判定を行う。（ここでは、（１）で登録した情報とは異なる結果が出たものと仮定する）基地局は判定の結果、登録済みの端末とは異なる端末からの情報であると判断し、受信データと共に否の端末判定信号を出力する。

（２’）基地局：要求信号

基地局は、端末判定の結果に従い端末の再確認を行うため、端末に対して認証要求信号を要求信号として出力する。

（1’）端末：基準信号送信

端末は、要求信号を受信するとそれに対応した動作を行う。ここでは基準信号を再度出力する。以下の手順は（1）～（3）と同様である。以上のような手続きを行うことで、伝搬環境の変化により誤った判定が起きる場合でも、再確認を行うことによって安定した通信を提供することが可能になる。

さらに、図４６の信号処理選択部４６０７では判定結果が異なる場合、情報処理部４６０５の処理を一時停止し、（1’）以降の再判定結果を待って情報処理の手順を決定することなどが考えられる。伝搬環境の変化に対応するためには、上記（3’）～（1’）の手続きとは別に、一定期間毎に基地局が登録した端末特定情報を更新することも考えられる。

また、（3）（3’）の通信信号の一部に基準信号を挿入することにより、基地局が安定した伝搬推定を行うことが可能となるため、その結果として安定した端末判定結果が得られるといった効果がある。このとき、基準信号は（1）で用いる基準信号と同一である必要はなく、通信内で一般的に用いられるパイロット信号や既知信号系列などで代用可能である。

以上説明した本発明では、例えば通信が開始されてから終了するまでのセッションにおいて基地局・端末間で認証が完了してからセッションが終了するまでの間の情報について有効性を付する事が可能になる。例えばインターネットで課金情報などを授受する際にセッション途中で別端末が途中で詐称した信号を発信し、通信に悪影響を与えることを防ぐことが可能であるといった大きな特長を有する。

以上の説明では、伝搬を推定するために基準信号を用いるとしたが、通信している環境下において誤り検出可能な信号系列であれば良い。このような信号系列としては、パイロット信号、既知信号、シンクワード信号、同期信号、同期ワード、プリアンブル信号、ミッドアンブル信号、ポストアンブル信号、リ

ファレンス信号、ユニークワード信号などが知られている。或いは、十分に復調エラーを保護された信号系列も用いることが可能であり、その例として例えば多値変調方式を通信している信号系列に含まれるＰＳＫ信号系列や、エラー訂正能力の高い方式で符号化された信号系列などが考えられる。

また、端末から基地局への通信の一部に端末を特定するＩＤを挿入し、その値と伝搬情報からの判定とを利用することも考えられる。

このように、本実施の形態１９の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、端末判定部４６０３は、現在通信している端末が自分が希望する通信相手であるのか否かを伝搬推定値より判定し、自分が希望する通信相手ではない場合には端末判定結果に基づいて受信データを復調しない等の受信データの処理を切り換えるので、より処理の安全性を保つことが出来ると共に、正常に認証できない端末によるデータ詐称などを防ぐことが可能となるため、非常に高いセキュリティを持った装置やシステムが構築できる。

（実施の形態２０）

図４８及び図４９は、伝搬パラメータに情報を多重するシステムにおいて具体的な通信フレームの設定方法を示した図である。なお、本実施の形態２０における通信装置は、図７と同一構成であるのでその説明は省略する。

本実施の形態２０は、便宜上下り回線を出力する装置を基地局、上り回線を出力する装置を端末として説明を行う。図４８は上り回線と下り回線との信号出力タイミングを説明した図である。図４８（ａ）は、セキュア情報を一方向で通信する場合であり、図４８（ｂ）は、セキュア情報を双方向で通信する場合である。なお、本実施の形態２０においては、基地局と端末とは送受信装置７００を備えているものとする。

最初に、一方向でセキュア情報を通信する場合について説明する。基地局は、端末に対して暗号化されていない通常の通信信号＃４８０１を送信している場合において、端末から基地局へ上り回線を用いて基準信号＃４８０２を含む

通信信号＃４８０３が送信されてきた場合には、基準信号＃４８０２に基づいて伝搬状態に応じた暗号鍵を選択し、選択した端末と共通の暗号鍵を用いて暗号化した暗号化通信信号＃４８０４を端末へ送信する。端末は、基準信号＃４８０２を含む通信信号を所定の周期にて基地局へ送信する。基地局は、端末から送信された基準信号＃４８０２を受信する度に暗号鍵が変更されていないか否かを確認し、確認後に暗号化信号＃４８０５を端末へ送信する。

次に、双方向でセキュア情報を通信する場合について説明する。基地局は、端末に対して基準信号＃４８０６を含む通信信号＃４８０７を送信する。端末は、基地局に対して基準信号＃４８０８を含む通信信号＃４８０９を送信する。基準信号＃４８０８を受信した基地局は、基準信号＃４８０８に基づいて伝搬状態に応じた暗号鍵を選択し、選択した暗号鍵を用いて暗号化した暗号化信号＃４８１０を端末へ送信する。一方、基準信号＃４８０６を受信した端末は、基準信号＃４８０６に基づいて伝搬状態に応じた暗号鍵を選択し、選択した暗号鍵を用いて暗号化した暗号化信号＃４８１１を基地局へ送信する。そして、基地局は暗号化した暗号化信号＃４８１２を端末へ送信する。

次に、図４９を用いて基準信号を送信するタイミングについて説明する。図４９はバースト構成の一例を示したものである。

図４９（ａ）のフレーム構成は、バーストが通信信号と基準信号とで構成されている。基準信号は、例えばパイロット信号を用いる。この様に構成することで、伝搬特性を推定するための信号と、データを伝送するための基準信号を同時に送信することが可能となり、効率の良いフレーム構成が実現可能となる。また、基準信号の一部或いは全部を２シンボル以上連続した信号で構成することにより、伝搬特性を推定する場合に、伝搬特性の変化量の少ないシンボルを利用して推定が可能となるため、精度の高い伝搬推定を実現可能という特長を有する。また、基準信号を一定の間隔でバースト全体に配置することで、高速フェージングなどによりバースト内で伝送特性が大きく変動しても基準信号を基にフェージング歪を補正出来るため高品質の伝送を実現可能となる。この

ような高速フェージング環境下では、各実施の形態で述べたような端末間で形成される伝搬特性を利用した通信は、実現が困難となるため、高速フェージング状態を検知して互いの端末が伝搬特性を利用した通信を行うか行わないかの切り替えを行うことも可能となる。

図４９（ｂ）のフレーム構成は、図４９（ａ）で示したフレーム構成の基準信号の一部或いは全部を基準信号１と基準信号２とすることとしたものである。この様に構成し、このバーストを送信する端末（端末１）が送信対象となる端末（端末２）に対して伝搬特性を利用して受信点において基準信号１の受信電力が基準信号２の受信電力より大きくなるように制御して通信を実施することで、送信対象となる端末２では受信電力の違いから基準信号１を判断し通信信号の基準として正しく復調することが可能となるが、他の端末では場所によって夫々の受信電力が異なるため正しく復調することが不可能となるといった特長を有する。また、端末２のアンテナの数がｎ個ある場合、各アンテナに対して基準信号１～基準信号ｎを多重する事も考えられる。この様にすることで基準信号１～ｎの伝搬パラメータに対して情報を重畳することで高度な通信を可能にする。また、端末２がｍ個ある場合、夫々の端末に対する通信を空間多重することにより周波数利用効率を向上させることも可能になる。（この場合、ｎとｍとの間にはｎ＞ｍの関係が成り立つ。）以上のようにすることで周波数利用効率の高いシステムを構築することが可能となる。

図４９（ｃ）のフレーム構成は、図４９（ａ）で示したフレーム構成の通信信号の一部或いは全部を通信信号１と通信信号２とすることとしたものである。この様に構成し、端末１が端末２に対して伝搬特性を利用して受信点において通信信号１の受信電力が通信信号２の受信電力より大きくなるように制御して通信を実施することで、送信対象となる端末２では受信電力の違いから通信信号１を判断し復調することが可能となるが、他の端末では場所によって夫々の受信電力が異なるため正しく復調することが不可能となると言った特長を有する。通信信号は、データ、データシンボル、変調シンボル、データ変

調シンボル、フリーシンボルまたはユーザシンボルなどとも呼ばれることもあり、通信データによって変調されるシンボルの事を示している。

このように、本実施の形態２０の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、基準信号の送信タイミングを変えるかまたは上り回線と下り下線を選択して基準信号を送信することにより、効率良く暗号化した信号を送受信することができる。

なお、本実施の形態２０においては、図４８（ｂ）、（ｃ）において、受信電力の違いに着目して説明したが伝搬パラメータの一例として説明したにすぎず、通信信号１（基準信号１）と通信信号２（基準信号２）との伝搬パラメータの差に情報を重畳することも考えられ、通信信号１と通信信号２を受信する端末２では通信信号１（基準信号１）を基準として伝搬パラメータの差を算出し、この結果を復調結果の一部或いは全部とすることも考えられる。また、本実施の形態２０においては、図４９（ｂ）では基準信号を多重する場合について説明し、図４９（ｃ）では通信信号を多重する場合について説明したが、当然基準信号と通信信号とを多重する事も可能であることは言うまでもない。

（実施の形態２１）

図５０は、伝搬パラメータに情報を多重するシステムにおいて具体的な通信フレームの設定方法を示した図である。なお、本実施の形態２１における通信装置は、図３６と同一構成であるのでその説明は省略する。

図５０は、符号分割多重（ＣＤＭ）のフレーム構成の一例を示したものである。

図５０（ａ）のフレームは、パイロット信号とデータ信号とで構成されている。パイロット信号は、データ信号の位相や振幅の基準を示したものである。受信装置はデータ信号の復調時に、このパイロット信号から求められた位相や振幅の情報を復調の基準とするほか、時間や周波数の同期・マルチパス状態などの伝搬状態を算出する。データ信号ではデータ１～ｎ（ｎは１以上の整数）を符号分割多重してある。ここで、データ１～ｎには符号１～ｍが割り当てら

れているものとする。端末１は推定した伝搬特性に応じてデータ１～ｎ夫々に対して伝搬パラメータ（ここでは受信電力とする）を制御する。この時、受信電力に情報を重畳させるようにして重み付けすると、端末２の受信端では、データ１～ｎの夫々の受信電力が制御された状態で受信される。これらの受信電力は符号１～ｍで逆拡散した信号振幅として得られるため、その振幅情報から重畳された情報を検出することが可能となる。ここでは、多重するデータ数をｎ、符号の種類をｍとしたが、ｎとｍとの間にはｎ≧ｍの関係が成り立つ。さらに端末１が制御する受信電力を０とすることでｎ＞ｍでの通信が可能となる。さらに様にｍ＝１の場合は、符号分割多重を行う必要はない。

図５０（ｂ）のフレームは、図５０（ａ）のフレーム構成とは異なり、データ１～ｎにパイロット信号を符号分割多重したことを特徴としたものであり、図５０（ａ）のフレーム構成と同様に伝搬パラメータに情報を重畳させて伝送することも可能である上、パイロット信号の位相や振幅を制御することも考えられる。

図５０（ｃ）のフレームは、データ１～ｎにパイロット１～ｍを符号分割多重したことを特徴としたものである。この構成を採ることにより、最大ｍ個のパイロット信号を夫々独立して制御可能となるため、例えばデータ１～ｊはパイロット１の位相や振幅を基準として変調され、データｊ＋１～ｋはパイロット２の位相や振幅を基準として変調される等により、高度な通信システムが構築可能となる。このようにすることで、複数の受信端末に対して、それぞれのパイロット信号とそれに対応したデータ信号とで独立に通信を行うことが可能であり、かつ夫々のパイロット信号は通信相手とする受信端末の受信端において正しい信号基準となるように制御されていることから、受信端末同士が他のデータ信号を受信し復調しようと試みても正常に復調できないと言った大きな特長が得られる。通信信号は、データ、データシンボル、変調シンボル、データ変調シンボル、フリーシンボルまたはユーザシンボルなどとも呼ばれることもあり、通信データによって変調されるシンボルの事を示している。

このように、本実施の形態２１の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、パイロット信号とデータを符号分割多重するので、干渉に強い暗号化信号の送受信を行うことができる。

なお、本実施の形態２１においては、パイロット信号を用いてデータ信号の位相や振幅の基準にすることとしたが、これに限らず、パイロット信号以外の基準信号を任意に選択することができる。

（実施の形態２２）

図５１は、本発明の実施の形態２２に係る通信装置である送受信装置５１００の構成を示す図である。送受信装置５１００は、図２に示す本実施の形態１に係る送受信装置２００において、直交周波数分割多重部５１０１を追加するものである。なお、図２と同一構成である部分には同一の符号を付してその説明は省略する。

切換部２１０は、送信信号が後述する直交周波数分割多重部５１０１にて直交周波数分割多重処理された後の送信信号が各サブキャリアに対して所望の配置となるように暗号化部２０９から出力される暗号化されたセキュリティデータと基準信号生成部２０８から出力される基準信号とを切り替えて変調部２１１へ出力する。

直交周波数分割多重部５１０１は、変調部２１１から入力した送信信号を直交周波数分割多重処理して送信部２１２へ出力する。即ち、直交周波数分割多重部５１０１は、変調部２１１から入力した送信信号を、パラレルデータ形式からシリアルデータ形式に変換して逆高速フーリエ変換した後にパラレルデータ形式からシリアルデータ形式に変換して送信部２１２へ出力する。直交周波数分割多重処理された送信信号は、各サブキャリアに振り分けて配置される。

図５２は、直交周波数分割多重（ＯＦＤＭ）のフレーム構成の一例を示したものである。縦軸は周波数、横軸は時間を表しており、１つの枡は１シンボル中の１サブキャリアを表している。

図５２（ａ）のフレームは、シンボル同期用のパイロット信号、データ復調

用の基準信号及びデータ送信用のデータ信号から構成されている。シンボル同期用のパイロット信号は、ＯＦＤＭシンボルの時間と周波数の同期を行うために用いられ、ヌルシンボルやショートワードシンボル、ロングワードシンボルなどが知られる。一方、データ副長用の基準信号は、伝搬歪により発生する周波数特性や伝搬遅延・位相回転などを補正するために挿入されるものであり、変調されるデータ信号の位相や振幅の基準を与える。フレーム内にこの基準信号を挿入することにより伝搬環境が変化したり、遅延プロファイルが変化したりする環境においても安定した通信を可能にする。本発明により、基準信号を伝搬特性に対応して、受信端における位相や振幅を制御して伝送する事により、設定した受信端以外の場所では正しい基準信号が得られないため、正しい復調を行うことが困難になると言った大きな特長を有する。

図５２（ｂ）のフレームは、図５２（ａ）のフレーム構成と同様にシンボル同期用のパイロット信号、データ復調用の基準信号及びデータ信号とからなっている。特定のシンボルで基準信号を送信する図５２（ａ）のフレーム構成に対して全シンボルの一部が基準信号となっていることから、シンボルに対応して基準信号を変化させることが可能となる。則ち、シンボルの切替時に伝搬特性を利用した制御係数を変化させて基準信号が示す位相や振幅の値を時々刻々と変化させることで、より複雑な制御が可能となりセキュリティシステムにおいては、高度なセキュリティが確保できるといった特徴を有する。また、基準信号は既知信号であることからパイロット信号としても利用することが可能であり、こうする事で環境の時間変化に対して補正がかけられるといった特徴を有する。

図５２（ｃ）のフレームは、図５２（ｂ）のフレーム構成の基準信号を時刻によって変化させることが特徴である。基準信号の位置が刻々と変化することで、基準信号やデータ信号に対して周波数ホッピングの効果が現れる。則ち、伝搬状態によるノッチによって一定のサブキャリアの電力が低くなったとしても信号パターンが切り替わるため、ノッチによる影響は一時的なものに抑え

られる。例えば、基準信号の箇所がノッチによって影響を受けてしまうとデータ信号に対して大きな影響がある上、フレーム構成２であれば伝搬状態が変化するまではその影響が続いてしまうが、本構成であれば基準信号の影響を限定的にすることが可能となる。通信信号は、データ、データシンボル、変調シンボル、データ変調シンボル、フリーシンボルまたはユーザシンボルなどとも呼ばれることもあり、通信データによって変調されるシンボルの事を示している。

このように、本実施の形態２２の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、直交周波数分割多重部５１０１は、暗号化されたデータ及びパイロット信号を直交周波数分割多重処理して各サブキャリアに配置するので、暗号化信号を送信する際の周波数利用効率を高くすることができる。

（実施の形態２３）

本実施の形態２３は、上位層の指示によりセキュリティ通信を行うか否かを決定する点を特徴とするものである。

図５３は、本実施の形態２３に係る送受信装置の構成を示す図である。なお、図７と同一構成である部分には同一の符号を付してその説明は省略する。

通信制御部５３０１は、通信時刻に応じて通信方法の切り換え・合成の制御を行う。即ち、通信制御部５３０１は、上位層５３０３からセキュア通信を行うための通信制御信号が入力した場合には、符号化部７０３から入力した伝搬情報を伝搬制御部７０１へ出力し、さらに受信部２０２へセキュア通信を行う旨の受信制御信号を出力するとともに送信部７０５へセキュア通信を行う旨の送信制御信号を出力する。一方、通信制御部５３０１は、セキュア通信を行わない旨の通信制御信号が入力した場合には、受信部２０２へセキュア通信を行わない旨の受信制御信号を出力するとともに送信部７０５へセキュア通信を行わない旨の送信制御信号を出力する。伝搬制御の方法については、セキュリティ通信を行う場合は他の実施の形態で示したような伝搬制御を行い、従来の通信方法を行う場合は伝搬制御をせずに通信したり、或いは伝搬制御として

指向性を絞って通信品質の向上を図る事も考えられる。

バッファ部５３０２は、送信データを一時的に保持して切換部２１０へ出力する。

上位層５３０３は、通信のレイヤ構造で言うＬ１より上位にあたる部位（データリンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層のうちのどれか）となる。上位層部では、受信データや送信データの入出力を行うと同時に、必要に応じて通信方法の選択が行われその制御信号を、それを通信制御信号として出力する。

本発明を用いた通信方法は、従来の通信方法と親和性が高く両者の通信方法を切り換えて利用することも可能である。この様にすることで、

（１）通信相手である通信装置がセキュリティ通信をサポートしているかどうか（２）アプリケーションが本発明の通信方法をサポートしているかどうか

（３）アプリケーションが本発明の通信方法を必要としているかどうか

（４）ユーザが本発明の通信方法を必要としているかどうか

などの状況に応じて従来の通信方法か、本発明を用いた通信方法かを切り換えることも可能である。更に、他の実施の形態でも述べたようにセキュリティ通信を必要とする場合でも、重要な情報だけをセキュリティ保護して通信を施すことで通信品質を確保出来ると言った事も考えられる。

次に、図５３に示す送受信装置の動作について、図５４を用いて説明する。

上位層部からセキュリティ通信を実施するように通信制御信号が出されると、通信制御部がセキュリティ通信用に伝搬制御を行うように送信・受信制御信号を出力する。（図中の（１）、（４））一方上位層部からセキュリティ通信を実施しないように通信制御信号が出されると、通信制御部がセキュリティ通信用に伝搬制御を行わないように送信・受信制御信号を出力する。（図中の（２）、（３）、（５））

このように、本実施の形態２３の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、通信制御部５３０１は、上位層５３０３の指示

により、伝搬推定値を用いて第１データの送受信を行う通信方式である重要な情報をセキュリティ保護したセキュリティ通信方法と従来の通信方式とを切り替えて送信するので、汎用性のある通信装置を提供することができる。

なお、本実施の形態２３においては、送信制御信号及び受信制御信号によって受信部２０２や送信部７０５の伝搬制御をＯＮ／ＯＦＦするとしたが、これに限らず、受信部２０２または送信部７０５のどちらかが従来の通信装置の該当部位と同一の構成である場合、その部位に対する制御信号は不要である。例えば、図１に示した通信装置の送信部１５２や、図７に示した通信装置に対応する通信装置の暗号受信部７０６などがこれに相当する。

（実施の形態２４）

本実施の形態２４は、アンテナ係数に秘匿情報を含めるようにする点を特徴とするものである。

図５５は、本実施の形態２４に係る通信装置である送信装置５５００の構成を示す図であり、図５６は、本実施の形態２４に係る通信装置である受信装置５６００の構成を示す図である。

最初に送信装置５５００について説明する。

変調部５５０１は、第２データを一時的に保持してチャネル数分のチャネル位相変調信号を合成部５５０２へ出力する。

合成部５５０２は、伝搬変調部５５０７より入力した変調アンテナ係数に従って変調部５５０１から入力した変調信号との合成演算が行われる。

送信部５５０３は、合成部５５０２から入力した合成信号を周波数変換及び電力増幅等する。

アンテナ５５０４は、対応する系列の信号を放射する。

伝搬特性格納部５５０５は、遅延プロファイル等の伝搬特性を格納してアンテナ係数算出部５５０６へ出力する。

アンテナ係数算出部５５０６は、アンテナ係数に代表される伝搬状態に情報を重畳するために、伝搬特性格納部５５０５から入力した伝搬特性に基づいて

アンテナ係数を算出する。アンテナ係数の求め方は様々であるが、特異値分解などが知られている。

伝搬変調部５５０７は、アンテナ係数算出部５５０６から入力したアンテナ係数と秘匿情報として送信する第１データを重畳して振幅変調した変調アンテナ係数を合成部５５０２へ出力する。

次に、受信装置５６００について説明する。

アンテナ５６０１は、受信ＲＦ信号を受信部５６０２へ出力する。

受信部５６０２は、アンテナ５６０１にて受信して入力した受信ＲＦ信号を電力増幅及び周波数変換等して復調部５６０３へ出力する。

復調部５６０３は、受信部５６０２から入力した各チャネル信号を復調してチャネル復調信号をアンテナ係数検出部５６０５とバッファ５６０４へ出力する。受信装置５６００では位相変調に振幅変調が加えられたＱＡＭ信号（或いは位相・振幅変調信号）が受信されることになるため、復調部５６０３は、受信信号を位相・振幅復調する。

バッファ５６０４は、復調部５６０３から入力したチャネル復調信号を一時的に保持して第２データを出力する。

アンテナ係数検出部５６０５は、復調部５６０３から入力したチャネル復調信号よりチャネル毎にアンテナ係数を検出し、検出したアンテナ係数情報を比較部５６０６へ出力する。

比較部５６０６は、アンテナ係数検出部５６０５から入力したアンテナ係数情報を符号化し、符号化したアンテナ係数情報の大きさを比較した結果を第１受信データとして出力する。なお、送信装置５５００及び受信装置５６００の動作は、受信電力の代わりにアンテナ係数を用いる以外は図３７と同一であるのでその説明は省略する。

本発明の伝搬特性に情報を重畳する場合、アンテナから出力される変調方式と受信装置が復調する変調方式が異なる点が大きな特徴である。換言すれば、アンテナから出力する信号の変調方式が、受信装置のサポートする変調方式と

異なるように設定することも可能である。このようにすることで、送信対象となる受信装置に対してのみ正しい変調信号となり、他の受信装置では正しい変調信号が得られないため、高度な秘匿性を確保できる。また、複数チャネルの信号におけるアンテナ係数差の情報に秘匿情報を含めることができるので、高いセキュリティが確保できるとともに、複数チャネルの信号を伝送することができるので、伝送効率を向上させることができる。

このように、本実施の形態２４の通信装置及び通信システムによれば、上記実施の形態１の効果に加えて、合成部５５０２は、伝搬変調部５５０７にて変調した第１データと変調部５５０１にて伝搬変調部５５０７とは異なる変調方式により変調した第２データとを合成し、送信部５５０３は、位相、振幅または周波数を組み合わせた変調方式にて第１データと第２データを送信するので、変調方式が異なる通信相手は復調することができないため、高いセキュリティを確保することができる。

なお、本実施の形態２４においては、アンテナ出力信号を位相変調とするとともに伝搬変調を振幅変調としたが、これに限らず、両者が同じ変調方式でも良く、また変調方式もこれに限ったものではない。それぞれは、周波数変調、位相変調、振幅変調、ＰＷＭ、ＰＡＭ、直交振幅変調、ＣＣＫ（Ｃｏｍｐｌｉｍｅｎｔａｒｙ　Ｃｏｄｅ　Ｋｅｙｉｎｇ）などが考えられる。

（実施の形態２５）

本実施の形態２５は、拡散処理した複数チャネルの信号にアンテナ係数情報を重畳してアンテナ係数情報を秘匿データとして取り出す点を特徴とするものである。

図５７は、本実施の形態２５に係る通信装置である送信装置５７００の構成を示す図であり、図５８は、本実施の形態２５に係る通信装置である受信装置５８００の構成を示す図である。なお、図５７及び図５８において、図５５及び図５６と同一構成である部分には同一の符号を付してその説明は省略する。

拡散符号格納部５７０１は、チャネル数分の拡散符号を格納して拡散部５７

０２へ出力する。

拡散部５７０２は、変調部５５０１から入力した第１データであるチャネルデータと拡散符号格納部５７０１から入力したチャネルに対応する拡散符号を畳み込み演算し周波数拡散を行って合成部５５０２へ出力する。

拡散符号格納部５８０１は、チャネル数分の拡散符号を格納して逆拡散部５８０２へ出力する。

逆拡散部５８０２は、拡散符号格納部５８０１から入力したチャネルに対応する拡散符号と受信部５６０２から入力した受信信号とを畳み込み演算により逆拡散しチャネル信号を復調部５６０３へ出力する。なお、送信装置５７００及び受信装置５８００の動作は、受信電力の代わりにアンテナ係数を用いる以外は図３７と同一であるのでその説明は省略する。

本発明の伝搬特性に情報を重畳する場合、アンテナから出力される変調方式と受信装置が復調する変調方式が異なる点が大きな特徴である。換言すれば、アンテナから出力する信号の変調方式が、受信装置のサポートする変調方式と異なるように設定することも可能である。このようにすることで、送信対象となる受信装置に対してのみ正しい変調信号となり、他の受信装置では正しい変調信号が得られないため、高度な秘匿性を確保できる。

このように、本実施の形態２５の通信装置及び通信システムによれば、上記実施の形態１及び実施の形態２４の効果に加えて、合成部５５０２は、伝搬変調部５５０７にて変調した第１データと変調部５５０１にて伝搬変調部５５０７とは異なる変調方式により変調して拡散処理した第２データとを合成し、送信部５５０３は、位相、振幅または周波数を組み合わせた変調方式にて第１データと第２データを送信するので、周波数利用効率の高いデータについて高いセキュリティを確保することができる。

なお、本実施の形態２５においては、アンテナ出力信号を位相変調とするとともに伝搬変調を振幅変調としたが、これに限らず、両者が同じ変調方式でも良く、また変調方式もこれに限ったものではない。それぞれは、周波数変調、

位相変調、振幅変調、ＰＷＭ、ＰＡＭ、直交振幅変調、ＣＣＫ（Ｃｏｍｐｌｉｍｅｎｔａｒｙ　Ｃｏｄｅ　Ｋｅｙｉｎｇ）などが考えられる。

（実施の形態２６）

本実施の形態２６は、アンテナ係数を制御することで一次変調に二次変調を重畳する点を特徴とするものである。

図６８は、本実施の形態２６に係る通信システムを示す図であり、図６９は送受に係る部位を詳細に示したものである。まず、図６８について説明する。

図６８で示すシステムでは、伝搬空間６８５２を介して通信端末Ａ６８５０と同一に構成された通信端末Ｂ６８５１とでなっている。なお、図６８では同一端末であるものとして示したが、この構成については同一端末である必要はない。

通信端末Ａ６８５０および通信端末Ｂ６８５１について説明する。

参照信号格納部６８０１は、時間同期、周波数同期や位相・振幅などの基準を与える参照信号を出力する。

変調部６８０２は、データ２（第２データ）を入力して所定の変調信号を生成し変調信号を出力する。

チャネル合成部６８０３は、変調信号とチャネル成分を抽出したチャネルパラメータ、データ１（第１データ）とを入力し、伝搬を通じてチャネル合成を行うように信号の重み付けを行い、送信ＲＦ信号を出力する。

チャネル解析部６８０４は、受信信号から抽出した伝搬係数を入力してこれを解析しチャネル合成するための係数を算出、出力する。

受信復調部６８０５は、受信ＲＦ信号を入力して、その伝搬係数をチャネル解析部６８０４に出力するとともに、復調してデータ１、２を出力する。

ＲＦ部６８０６は、送信ＲＦ信号をアンテナ６８０７へ出力するとともに、アンテナ６８０７で受信した信号を入力して受信復調部６８０５へ受信ＲＦ信号を出力する。

アンテナ６８０７は、対応する系列の送信ＲＦ信号を放射、あるいは受信し

た受信ＲＦ信号を受信復調部６８０５へ出力する。

スイッチ６８０８は、チャネル合成部６８０３に出力する変調信号を参照信号格納部６８０１からの信号とするか、変調部６８０２からの信号とするかを選択し、出力する。

制御部６８０９は制御信号を入力し、チャネル合成部６８０３、チャネル解析部６８０４、受信復調部６８０５、スイッチ６８０８の制御を行う。具体的には、実施の形態２３に記載したように上位層からの制御信号を受け、秘匿通信を行うか否かの設定を行ったり、実施の形態１などに記載の通信手順に応じて伝搬推定信号の出力や、規定されている通信フレームに準じた動作の制御を行う。

送受信部分の詳細を記載した図６９について説明する。図６９は、図６８の一部を詳細に示したものであり、同様の構成部位については同一符号を付してある。ここでは、各部位の説明は省略し、動作の詳細について説明する。

データ（データ１～ｎ）を入力した変調部６８０２はそれぞれ対応するデータから変調信号１～ｎを生成し、チャネル合成部６８０３へ出力する。チャネル合成部６８０３には、変調部６８０２から変調信号を入力するとともに、チャネル解析部６８０４からチャネルパラメータをアンテナ係数として入力する。チャネル解析部６８０４は、制御信号とＲＦ部６８０６で受信した受信信号を入力し、受信信号系列と参照信号などの既知信号系列などを利用して位相や振幅、遅延分散など伝搬特性の特徴を抽出しそのチャネルパラメータをチャネル合成部６８０３へと出力する。

チャネル合成部６８０３はチャネルパラメータと変調信号とからアンテナ系列に対応したアンテナ係数を算出する。また、制御信号により伝搬制御が必要であれば、このようにして算出したアンテナ係数と、変調信号とを掛け合わせ重み付けした送信信号を対応するＲＦ部６８０６へ出力し、ここで電力増幅されてアンテナ部６８０７から放射される。

一方、伝搬制御が必要でない場合は、通信に適した（即ち受信点で最大感度

となるような信号になるよう）制御を行ったり、重み付け係数を予め設定されてある値にセットしたり、あるいは１つ以上の係数を０にセットしたりする。通信に適した制御を行った場合、通信品質が向上されるという特長がある。重み付け係数を予め設定してある値にセットする場合、たとえば通信環境がほぼ固定であり、指向性が予め設定できるような状況であれば複雑な制御を行わずに高い通信品質が向上するといった特長がある。このように事前に指向性を予め設定できない場合は、全てを同一値に設定することでトータルの出力電力を向上させることとなり通信品質の向上につながる。重み付け係数の一部を０にセットする場合、出力電力の抑制になり、消費電力の低減が可能になる。

重み付け操作に関しては図３５に示したような構成で可能である。ここで、重み付けされる変調信号とアンテナ係数の算出時に用いる変調信号とを明確に分離することで、情報の階層化が容易に実現できることは明らかである。（このとき前者を一次変調、後者を二次変調と呼ぶことにする）このようにするとき、変調信号１～ｋを一次変調、変調信号ｋ＋１～ｎを二次変調とすることで可能である。たとえば実施の形態１７で示したように、１つの変調信号以外はすべて電力が０となるように制御するという方式の場合、二次変調として（１、０）の変調信号に一次変調した変調信号１～ｋを、同様に二次変調として（０、０）の変調信号に一次変調した変調信号ｋ＋１～ｎを適用しているとみなすことも可能である。このように二次変調である変調信号のパターンが少ない場合、アンテナ係数をパターン数だけ用意しておきこれを二次変調に対応するデータで切り替えることで実現が可能である。

ここで、アンテナ係数は数式３４で与えられる。

$$H \cdot W(x) = x \qquad (34)$$

数式３４でのｘは二次変調で情報を重畳する成分であり、ＡＳＫであれば振幅、ＰＳＫであれば位相、ＦＳＫであれば周波数となる。

こうして放射された電波は、伝搬空間６８５２を介して通信端末Ｂ６８５１のアンテナ６８０７で受信される。この信号はチャネル合成部６８０３によっ

てチャネルパラメータが重畳されており、受信信号Ｓｒｘは一次変調信号Ｓｔ＿１、二次変調信号Ｓｔ＿２、チャネル特性Ｈ、およびアンテナ係数Ｗを用いて数式３５のように表すことが可能である。

Ｓｒｘ　＝　Ｈ・Ｗ（Ｓｔ＿２）・Ｓｔ＿１　　（３５）

数式３４を用いることで次式が得られる。

Ｓｒｘ　＝　Ｓｔ＿２・Ｓｔ＿１　　（３６）

数式３６で示された通り、通信端末Ｂ６８５１の受信端において、一次変調信号と二次変調信号とが掛け合わされた信号として受信信号が得られる。例えば一次変調をＰＳＫ変調、二次変調をＡＳＫ変調とすることで、受信復調部６８０５では、位相成分を検波することで一次変調に対応するデータ２を、振幅成分を検波することで二次変調に対応するデータ２を復調することが可能となる。

以上の説明を、図７０を用いて更に詳細に説明する。

図７０は、図６９をより具体的に示したものであり、図中の７０５０～７０５２に信号のコンスタレーションを記述してある。

重み付け乗算部７００１は、一次変調信号とアンテナ係数とを乗算した重み付け送信信号を出力する。

係数格納部７００２は、チャネル解析部６８０４が算出したチャネルパラメータを入力し、これを基本係数として保持する。保持した基本係数は二次変調信号に応じて係数をアンテナ係数に変換され出力される。このとき、上述の通り二次変調のパターンが少ない場合は、基本係数をそのパターン数用意しておき、二次変調に対応するデータ１に応じてアンテナ係数を切り替えることで容易に実現が可能となる。

ここで、一次変調をＱＰＳＫ、二次変調をＡＳＫとして説明する。信号７０５０ａは、ＱＰＳＫのコンスタレーション、信号７０５０ｂはＡＳＫのコンスタレーションを示している。

チャネル合成部６８０３では、係数格納部７００２から出力されたアンテナ

係数を用いて一次変調信号の重み付けを行い、対応するアンテナ６８０７へ重み付け送信信号を出力する。このアンテナ係数は、二次変調のシンボル‘ｓｐａｃｅ’と‘ｍａｒｋ’では、位相・振幅とも異なるため、一次変調信号が４つの信号点を有していたのに対して、それぞれの重み付け送信信号では８つの信号点を有していることになる。

ここで、二次変調信号の‘ｓｐａｃｅ’、‘ｍａｒｋ’に対するアンテナ係数は、位相・振幅が異なることとしたが、どちらかを一定値として固定することも可能である。振幅を一定にした場合、各アンテナから供給する電力が等しくなるといった特長を有する。位相を一定にした場合、重み付け乗算部７００１の構成が容易になるといった特長を有する。

信号７０５２は、伝搬空間６８５２を介して通信端末Ｂ６８５１で受信された信号を示しており、数式３６で示されたように、ＱＰＳＫにＡＳＫを重畳した８－ＡＰＳＫ信号のようになる。受信復調部６８０５は、位相を検波することで、データ２を、振幅を検波することでデータ１を復調することが可能である。

この様に本実施の形態２６によると、アンテナ係数を制御することで一次変調に二次変調を重畳し、この変調信号は受信点でのみ正しい変調信号を形成することから秘匿性の高い通信を可能にすることを特長とするものである。

（実施の形態２７）

本実施の形態２７は、上位層の通信において物理層での秘匿通信の制御を行う通信プロトコルについて記載したものである。

図５９は、実施の形態２７に用いる通信システムを示したものである。

通信システムは、通信端末Ａ５９５０と通信端末Ｂ５９５１が伝搬空間５９５２を介して通信を行っている。ここで、通信端末Ａ５９５０と通信端末Ｂ５９５１は同一の構成でなっている。

通信端末Ａ５９５０について説明する。

上位層４７５０はアプリケーション（端末外部からの場合や端末内部の場合

が考えられる）と受信情報と送信情報を授受し、送信データを送信部１５２、制御信号を通信制御部４７０１へ出力し、受信データを受信復調部１５０から入力する。

受信復調部１５０は、アンテナ１０１から受信ＲＦ信号を入力し、それを復調して受信データを出力する。

送信部１５２は、送信データを入力し変調信号を生成して送信ＲＦ信号をアンテナ１０１へ出力する。

通信制御部４７０１は、制御信号を入力し送信部１５２へ送信制御信号を、受信復調部１５０へ受信制御信号を出力する。また、受信復調部１５０から伝搬パラメータを入力し、送信部１５２へ伝搬パラメータを出力する。

アンテナ１０１は、送信部１５２から送信ＲＦ信号を入力しこれを放射し、受信した受信ＲＦ信号を受信復調部１５０へ出力する。

通信において必須となるチャネル制御や時間制御などの通信制御は通信制御部４７０１が行うが、それに加えて上位層からのコマンドは、制御信号を介して通知される。コマンドを受けた通信制御部４７０１は、送信制御信号や受信制御信号を通じて物理層のコマンド発行や秘匿通信制御などを行う。

以上の構成に基づいて、通信手順について図６１を用いて詳細に説明する。ここでは、実施の形態１で説明した秘匿通信に基づいて説明するが、これに限らず他の実施の形態で説明した秘匿通信についても適用可能であることは言うまでもない。

（０）初期化

通信端末Ａ５９５０および通信端末Ｂ５９５１は、電源投入時や通信開始時などで、所定の手順に基づき初期状態に設定するため、上位層から初期化の制御信号を出力する。

（０．ａ）、（０．ｂ）上位層から受けた制御信号に基づき、通信端末Ａ５９５０は物理層に関する設定状態を初期化する。

（１）セキュア情報送信

（１．０）通信端末Ａのアプリケーションが上位層にセキュア情報とそれを送信する要求を出力する。

（１．１）通信端末Ａの上位層はセキュア送信要求を受けると、物理層に対してセキュア情報とともにセキュア送信コマンドを発行する。

（１．２）通信端末Ａの物理層はセキュア送信要求コマンドを受けると、端末Ａ・Ｂ間での通信タイミングに合わせてセキュア通信コマンドを端末Ｂへ送信する。

（１．３）通信端末Ｂの物理層では、セキュア通信コマンドを受信すると、通信タイミングに従ってセキュア通信要求を伝搬推定用信号とともに通信端末Ａへ送信する。

（１．４）通信端末Ａの物理層では、セキュア通信要求を受信すると伝搬推定用信号から伝搬を推定し、伝搬パラメータを算出する。さらに伝搬パラメータを用いて（１．２）で入力したセキュア情報を、秘匿通信方法を用いて通信端末Ｂへ送信する。

（１．５）通信端末Ｂの物理層では、秘匿通信方法を用いて伝送されたセキュア情報を受信・復調し、その情報を上位層へ出力する。

（１．６）通信端末Ｂの上位層は物理層から出力されたセキュア情報を、アプリケーションへ出力する。

以上の一連の動作により、通信端末Ａのアプリケーションから通信端末Ｂのアプリケーションへセキュア情報が本発明の秘匿通信を用いて伝送される。本手順に従うことで、アプリケーション同士での通信手順を最も簡単に送信することが可能である。

以上の動作において、物理層における実際の通信信号について図６４を用いて説明する。図中で網掛けされた部分は、通信端末Ｂから通信端末Ａへの信号、他は通信端末Ａから通信端末Ｂへの信号を示している。セキュア通信コマンドが発行されると（１．２）、所定の間隔（Ｔｇｕａｒｄ）後にセキュア通信要求が伝搬用推定信号とともに受信される（１．３）。この伝搬用推定信号を用

いて算出した伝搬パラメータに基づき、セキュア通信が実行される（１．４）。

ここで、図中に示した時間について説明する。

Ｔｇｕａｒｄは通信信号の衝突を避けるために設けられた時間であり、一般にサポートする通信距離から求められる。

Ｔａｃｃｅｓｓはセキュア通信コマンドを発行してからセキュア通信が完了するまでの時間を表しており、上位層ではセキュア通信を行う際にこの値を用いて通信状態の管理を行うことが可能である。

Ｔｒｅｐｌｙはセキュア通信要求（伝搬推定用信号）が与えられてからセキュア通信が終了するまでの時間である。他の実施の形態でも示している通り、本発明は伝搬パラメータを通信に用いているため、伝搬環境に変化がないことを前提としており、伝搬環境に変化が起きた場合通信品質の劣化を招く。この影響について図７２～７４を用いて説明する。

図７２は、伝搬パラメータの直交性の時間的変化を表しており、所定の時刻における伝搬環境からの変化を直交性という指数で表現したものである。縦軸は指数の大きさを、横軸はシンボル時間を示している。すなわち特定の時刻（ｔ＝０）の伝搬状況から特異値分解で求めた直交ベクトルと実際の伝搬状況との直交度合いを示しており、０であれば、伝搬パラメータと伝搬状況が一致していることを示す指数である。この値は、伝搬パラメータと伝搬状況のずれを示すものであるが、この値が０．３（点線で図示）を超える付近で特性が大幅に劣化する。

図７３、図７４は通信品質をビットエラーレート（ＢＥＲ）で表したものであり、通信変化の多様性を鑑み、８通りのフェージングパターンにおける通信品質を示したものである。図７３では指数が０．２５付近の通信状態を示しており、図７４では指数０．３５付近の通信状態を示している。図７３では全ての通信でＢＥＲが０．０１以下まで落ちているのに対して、図７４では、ほとんどの通信でＢＥＲが０．０１以上に留まっている。ＢＥＲが０．０１以下である場合は、誤り訂正で情報の復元が可能であることを考えると、指数が０．

３以下であることが本発明の秘匿通信の大きな目安となる。

図７２に示したｆｄはフェージングピッチを表しており、次式で与えられる。

ｆｄ＝（Ｓｍａｘ／Ｃ）＊Ｆｃ／Ｆｂａｕｄ　　（３７）

ここで、Ｓｍａｘは最大移動速度、Ｃは光速、Ｆｃはキャリア周波数、Ｆｂａｕｄはシンボルレート周波数である。こうして求められた値をｆｄ＝１／ｎとおくと、図より分るとおり凡そｎ／４～ｎ／３（シンボル時間）付近で０．３を超えていることが分る。即ち、安定した通信を行うためにはＴｒｅｐｌｙ＜ｎ／４（シンボル時間）を満たす必要がある。ここで無線ＬＡＮの規格を考えてみる。通信中の最大移動速度を３０ｋｍ／ｈ、キャリア周波数を２．４５ＧＨｚとすると、式３６からＴｒｅｐｌｙを満足するための値が求められる。（ｆｄとＴｒｅｐｌｙとがＦｂａｕｄによって規定されるため、Ｆｂａｕｄは相殺される）

Ｔｒｅｐｌｙ＝Ｃ／Ｓｍａｘ／Ｆｃ／４　　（３８）

上記条件を代入すると、Ｔｒｅｐｌｙが約３．５ｍｓ以下である場合に高い通信品質での通信が可能になる。

このようにＴｒｅｐｌｙの値に制限があるため、同一周波数帯を用いて複信を行うＴＤＤ（Ｔｉｍｅ　Ｄｉｖｉｓｉｏｎ　Ｄｕｐｌｅｘ）通信において、Ｔａｃｃｅｓｓ内に他の通信端末からのアクセスを禁止することが効果的である。即ちＴａｃｃｅｓｓをＴｒｅｐｌｙよりも大きな値（たとえば１０ｍｓ）に設定しておき、この期間は秘匿通信をおこなう端末同士のみが通信リソースを占有するように上位層が制御することが考えられる。

また、伝送する情報が多い場合、手順（１．３）、（１．４）を繰り返すことで、多くの情報伝送にも対応できる。この場合、先に述べたＴａｃｃｅｓｓも通信料に対応して長く確保することが望ましい。

次に、セキュア情報を要求する場合の手順について図６２を用いて説明する。

（０）初期化

前述の初期化と同一の作業を行う。

（2）セキュア情報受信

（2．0）通信端末Aのアプリケーションが上位層にセキュア情報受信の要求を出力する。

（2．1）通信端末Bの上位層はセキュア情報受信要求を受けると、物理層に対してセキュア受信コマンドを発行する。

（2．2）通信端末Bの物理層では、セキュア受信コマンドを受信すると、通信タイミングに従ってセキュア通信要求を伝搬推定用信号とともに通信端末Bへ送信する。

（2．3）通信端末Bの物理層では、セキュア通信要求を受信すると伝搬推定用信号から伝搬を推定し、伝搬パラメータを算出する。同時に上位層に対して情報要求コマンドを発行する。（物理層で管理された情報であれば上位層へのコマンド発行は行わず(2．4）（2．5）は不要。一方上位層で管理された情報であれば（2．4）は不要。）

（2．4）通信端末Bの上位層では、物理層からの情報要求コマンドを受けてアプリケーションから情報を入手する。

（2．5）通信端末Bの上位層では、セットした情報とともに情報応答コマンドを物理層に対して発行する。

（2．6）通信端末Bの物理層では、（2．4）で推定した伝搬パラメータを用いて、入手した情報を秘匿通信方法により通信端末Aへ送信する。

（2．7）通信端末Aの物理層では、秘匿通信方法を用いて伝送されたセキュア情報を受信・復調し、上位層へ出力する。

（2．8）通信端末Aの上位層は物理層から出力されたセキュア情報を、アプリケーションへ出力する。

以上の一連の動作により、通信端末Aのアプリケーションが通信端末Bに対してセキュア情報を要求し、通信端末Bから通信端末Aに対してセキュア情報を伝送することが可能になる。本手順に従うことで、セキュア情報を最も簡単な手順で受信することが可能である。

以上の動作において、物理層における実際の通信信号について図６５を用いて説明する。図中で網掛けされた部分は、通信端末Ａから通信端末Ｂへの信号、他は通信端末Ｂから通信端末Ａへの信号を示している。

セキュア通信要求が伝搬用推定信号とともに発行されると（２．２）、所定の間隔（Ｔｇｕａｒｄ）後、この伝搬用推定信号を用いて算出した伝搬パラメータに基づき、セキュア通信が実行される（２．６）。

時間の説明は図６４と同様であるため省略する。

先に述べたとおり、Ｔｒｅｐｌｙの時間に制約がある場合、（２．３）による情報がすぐに求められない場合が考えられる。この場合に有効な通信手順について図６３を用いて説明する。

（０）初期化

前述の初期化と同一の作業を行う。

（３）セキュア情報受信

（３．０）通信端末Ａのアプリケーションが上位層にセキュア情報受信の要求を出力する。

（３．１）通信端末Ｂの上位層はセキュア情報受信要求を受けると、物理層に対してセキュア受信コマンドを発行する。

（３．２）通信端末Ｂの物理層では、セキュア受信コマンドを受信すると、通信タイミングに従って情報準備要求を通信端末Ｂへ送信する。

（３．３）通信端末Ｂの物理層では、情報準備要求を受信すると、上位層に対して情報要求コマンドを発行する。（物理層で管理された情報であれば上位層へのコマンド発行は行わず(３．４）（３．５）は不要。一方上位層で管理された情報であれば（３．４）は不要。）

（３．４）通信端末Ｂの上位層では、物理層からの情報要求コマンドを受けてアプリケーションから情報を入手する。

（３．５）通信端末Ｂの上位層では、セットした情報とともに情報応答コマンドを物理層に対して発行する。

（３．６）通信端末Ｂの物理層では、情報がセットされたことを情報応答コマンドで通知されると、通信端末Ａに対して情報準備完了を通知する。

（３．７）通信端末Ａの物理層では、通信端末Ｂからの情報準備完了通知を受信すると、通信タイミングに従ってセキュア通信要求を伝搬推定用信号とともに通信端末Ｂへ送信する。

（３．８）通信端末Ｂの物理層では、セキュア通信要求を受信すると伝搬推定用信号から伝搬を推定し、伝搬パラメータを算出する。次に推定した伝搬パラメータを用いて、入手した情報を秘匿通信方法により通信端末Ａへ送信する。

（３．９）通信端末Ａの物理層では、秘匿通信方法を用いて伝送されたセキュア情報を受信・復調し、上位層へ出力する。

（３．１０）通信端末Ａの上位層は物理層から出力されたセキュア情報を、アプリケーションへ出力する。

以上の動作において、物理層における実際の通信信号は前述図６５の説明と同一であるので省略する。

以上の動作により、アプリケーションが特に通信状態を意識することなく秘匿通信を行うことが可能であるが、アプリケーションによっては特定の情報を秘匿通信で授受したり、受けた情報が秘匿通信されているかの情報が必要な場合もある。この様な場合、図６０に示されているように上位層４７５０での処理において例えば（１．０）、（２．０）、（３．０）、（１．６）、（２．８）、（３．１０）などのステップでアプリケーションと情報を授受する際に、情報の属性として秘匿通信を用いた事を示すフラグを付しておくことで、アプリケーションがより柔軟な処理が出来ると言った特長を有する。

この様に、本実施の形態２７を用いることで、上位層から物理層での効率的な秘匿通信の制御を可能にし、安定した通信プロトコルを提供する。

（実施の形態２８）

本実施の形態２８は、実施の形態１７、１８で説明した発明をさらに拡張して、送信端末が有する送信アンテナの本数を見かけ上多くすることを可能にし、

秘匿性を向上させることを特徴とする。

本実施の形態で用いる通信システムを図７７に示す。

通信端末Ａ７７５０と通信端末Ｂ７７５１はチャネル７７５２を介して通信を行っている。また、通信端末Ａ７７５０は１つの送受信アンテナ素子を、通信端末Ｂは４つの送受信アンテナ素子を有している。

まず、通信端末Ａ７７５０について説明する。

変調部７７０１はデータを入力し、それを変調した変調信号を出力する。

バッファ７７０２は変調信号を入力・保持したバッファド変調信号をチャネル合成部７７０３へ出力する。

チャネル合成部７７０３は変調信号にチャネルパラメータを用いて合成し、送信信号を送信部７７０４へ出力する。

送信部７７０４は送信信号を周波数変換、電力増幅し、送信ＲＦ信号をアンテナ７７０５へ出力する。

アンテナ７７０５は送信ＲＦ信号を放射し、受信した受信ＲＦ信号を受信部７７０６へ出力する。

受信部７７０６はアンテナ７７０５から入力した受信ＲＦ信号からベースバンド信号をチャネル推定部７７０７へ出力する。

チャネル推定部７７０７は受信部７７０６から入力したベースバンド信号からチャネル７７５２の特性を推定し、推定チャネル情報を出力する。

チャネル解析部７７０８は推定チャネル情報を入力し、所定の解析方法を用いてチャネルパラメータを算出し、出力する。

次に、通信端末Ｂ７７５１について説明する。

アンテナ７７０９は送信ＲＦ信号を入力しこれを放射すると共に、受信した受信ＲＦ信号を送信部７７１０へ出力する。

受信部７７１０は受信ＲＦ信号からベースバンド信号へ変換しバッファ７７１１へ出力する。

バッファ７７１１はベースバンド信号を一時保持し、所定時間だけずらした

信号を選択合成部に出力する。

選択合成部７７１２は時間差のついた信号を合成し、合成信号を出力する。

復調部７７１３は合成信号を入力し、これを復調してデータを得る。

参照信号格納部７７１４はチャネル７７５２を推定するための参照信号を格納し出力する。

アンテナ選択部７７１５は参照信号を入力し、これを選択されたアンテナに送信信号として出力する。

送信部７７１６は、送信信号を入力し送信ＲＦ信号を対応するアンテナ素子７７０９へ出力する。

ここで、通信伝搬路のチャネルをｈ１、ｈ２、ｈ３、ｈ４で構成されるチャネルマトリクスＨとして考える。通信端末Ａ７７５０が通信端末Ｂ７７５１からの参照信号を用いて伝搬を推定するが、このとき通信端末Ａ７７５０が通信端末Ｂ７７５１の各アンテナとの係数を測定できるように、夫々のアンテナから直交した信号を出力する。ここでは、その代表として時分割で参照信号を出力するものとする。こうすることで、通信端末Ａはｈ１、ｈ２、ｈ３、ｈ４を測定することが可能になる。

則ち、参照信号格納部７７１４から出力された参照信号をアンテナ選択部７７１５が順次出力するアンテナを切り換える。この様にして出力された送信信号は送信部７７１６で増幅され対応するアンテナから放射される。

通信端末Ａでは、アンテナ７７０５で上記参照信号を受信すると受信ＲＦ信号が受信部７７０６へ入力され順次ベースバンド信号へと変換される。チャネル推定部７７０７ではベースバンド信号を入力し参照信号を用いてチャネルの推定が行われ、チャネル情報を出力する。チャネル情報はチャネル解析部７７０８に入力され、その解析が行われる。ここでは実施の形態１８で説明した特異値分解を用いて説明する。特異値分解で得られた特異値ベクトルＶは、特異値が非０の特異ベクトルと特異値が０のゼロベクトルとに分離できる。ここで各ベクトルをｖ１～ｖ４、ｖ１を特異ベクトル、ｖ２～ｖ４をゼロベクトル、

特異値をλとする。またベクトル要素をｖｎ＝（ｖｎ１～ｖｎ４）（ｎ＝１..４）と定義する。これら特異ベクトルとゼロベクトルをチャネルパラメータとして出力する。

変調部７７０１は４系列のデータを入力し、所定の変調方式に則り変調信号を４系列生成し出力する。この変調信号をｄ１～ｄ４とし、ｄ１を通信用変調信号、ｄ２～ｄ４を疑似変調信号とする。バッファ部７７０２は、４系列の変調信号を入力しこれを保持する。バッファ部７７０２は４タイムスロット分同一の信号を保持し続ける。

最初のタイムスロットにおいて、チャネル合成部７７０３は４系列の変調信号とチャネルパラメータを入力し、以下の演算を行う。

$$DS1=\Sigma(vn1\cdot dn) \qquad (39)$$

（ｎはΣ変数とする、以下同様）

この様にして得られた送信信号を送信部７７０４へ出力する。

以下同様にｋ番目タイムスロットにおいて、チャネル合成部７７０３は変調信号ｄ１～４を入力し以下の演算を行う。

$$DSk=\Sigma(vnk\cdot dn) \qquad (40)$$

こうして出力された４タイムスロット分の送信信号は、伝搬路７７５２を介して通信端末Ｂ７７５１で受信される。通信端末Ｂ７７５１の受信処理の詳細を図７８に示す。各アンテナで受信した受信ＲＦ信号は対応する受信部７７１０によってベースバンド信号に変換され出力される。ベースバンド信号はバッファ部７７１１によって一時保持される。ここでは４タイムスロット分×４アンテナ系列で１６のバッファを表記してある。上記動作によって４タイムスロット分、バッファ部７７１１で蓄えられた信号を夫々Ｓｒｘ１１～４４とする。この信号は、チャネル要素ｈ１～ｈ４、チャネルパラメータ要素ｖ１１～ｖ４４、変調信号Ｓｔ１～４を用いて以下のように表現できる。

$$Srxjk=hj\cdot\Sigma(vnk\cdot dn) \qquad (41)$$

ここで、図６８に図示したように、Ｓｒｊ＝Ｓｒｘｊｋ（ｊ＝ｋ、ｊ＝１..

４）の信号について注目すると次式が得られる。

$$Srj = hj \cdot \Sigma (vnj \cdot dn) \qquad (42)$$

また、ΣＳｒｎは行列Ｈ、Ｖ、Ｄを用いて次式で与えられる。

ここでＤは［ｄ１　ｄ２　ｄ３　ｄ４］Ｔである（ＡＴはＡの転置行列）。

$$\Sigma Srn = H \cdot V \cdot D = \lambda d1 \qquad (43)$$

以上のような操作により、通信端末Ａ７７５０が送信しようとした変調信号ｄ１が得られ、その他の変調信号はキャンセルされることが分かる。復調部７７１３はこうして得られた信号をそのまま復調すれば、データが得られる。

ここで、第３者がこれを復調しようとしても他の実施の形態と同様、チャネルパラメータが不明であるため、ｄ１を分離することが出来ず復調できない。この様にすることで、受信・復調には特別な演算を必要とせず秘匿通信を実現できると言った大きな特長がある。

以上説明したことの通信信号について、図６７、７５を用いて説明する。

図中の網掛けは通信端末Ｂ７７５１から通信端末Ａ７７５０へ出力される信号を示しており、他は通信端末Ａ７７５０から通信端末Ｂ７７５１へ出力される信号を示している。

図中に示したように、セキュア通信要求信号と共に、伝搬推定用信号が出力される。本実施の形態では、タイムスロットを通信端末Ｂ７７５１のアンテナ素子数だけ設けて送信するとしたが、前述の通り各アンテナ要素から出力される信号が直交していればこれに限ったものではない。図中に示したＰ１～Ｐ４は対応するアンテナからそれぞれ出力される既知信号であり、これに基づいて通信端末Ａ７７５０のチャネル推定部７７０７は伝搬路を推定する。次に、通信端末Ａ７７５０は、秘匿通信を行う際、４つのタイムスロットを用意して（ＤＳ１～ＤＳ４）式４０で与えられる信号を送信することで、秘匿通信は行われる。

以上の説明に於いて、通信端末Ａ７７５０におけるアンテナ７７０５の要素数を１、通信端末Ｂ７７５１におけるアンテナ７７０９の要素数を４として説

明したが、これに限ったものではない。本発明は通信端末Ａ７７５０の要素数をｍ、通信端末Ｂ７７５１の要素数をｎとしたときｍ＜ｎ場合に、より高度の高い通信方式を提供するものである。ｍが２以上である場合、ｎのうちｋ（ｋ＜ｍ）であるようなアンテナ選択を行い、他の実施の形態で示したような秘匿通信も可能であるが、本発明はチャネル要素数を最大に取って秘匿通信が行えることから、最も高度な通信保護が為されていると言える。

この様に、本実施の形態２８を用いることで、アンテナ要素数（ｍ）が少ない通信端末がアンテナ要素数（ｎ）の多い通信端末に対して、最も高度な通信保護を可能とすることが特長であり、特にｍが１の場合に大きな効果を発揮する。

上記実施の形態１～２８においては、ハードウェアの構成により伝搬環境に応じた秘匿情報を取得することとしたが、これに限らず、プログラム等を用いたソフト上の処理により伝搬環境に応じた秘匿情報を取得するようにしても良い。この場合は、ＣＤ－ＲＯＭ等の記憶媒体に記憶させたプログラム等やネットワークを介して伝送されてきたプログラム等の任意の方式により取得したプログラム等を用いることが可能である。

以上説明したように、本発明によれば、伝搬状態に応じたデータを取り出すことができるので、大きな通信システムの変更をすることなしに高いセキュリティを確保することができる。

本明細書は、２００２年２月２８日出願の特願２００２－０５４０６４、２００２年５月７日出願の特願２００２－１３２０６８及び２００３年２月２５日出願の特願２００３－４８３６４に基づくものである。この内容をここに含めておく。

産業上の利用可能性

本発明は、ディジタル通信に用いられる技術であって、特にセキュリティに関する技術に用いるに好適である。

請求の範囲

1．通信相手から送信された信号を用いて伝搬環境を推定する伝搬環境推定手段と、前記伝搬環境推定手段により得られた推定値を用いて第1データを取得する第1データ取得手段と、を具備することを特徴とする通信装置。

2．前記第1データ取得手段にて取得した前記第1データを用いて受信信号を復号化することにより第2データを取得する復号化手段を具備することを特徴とする請求の範囲1記載の通信装置。

3．前記伝搬環境推定手段により得られた前記推定値を符号化する符号化手段を具備し、前記第1データ取得手段は、符号化した前記推定値の符号化パターンより前記第1データを取得することを特徴とする請求の範囲1記載の通信装置。

4．チャネル毎に求めた前記推定値をチャネル毎に互いに比較する比較手段を具備し、前記第1データ取得手段は、前記比較手段の比較結果に基づいて前記第1データを取得することを特徴とする請求の範囲1記載の通信装置。

5．通信相手との間で互いに既知である基準信号を格納する格納手段を具備し、前記伝搬環境推定手段は、前記基準信号と前記信号との相関を求めて前記推定値としての遅延プロファイルを作成し、前記第1データ取得手段は、遅延プロファイルと第1データとが対応付けられた参照テーブルを用い、当該参照テーブルから前記伝搬環境推定手段により作成された遅延プロファイルに対応した第1データを読み出すことで前記第1データを取得することを特徴とする請求の範囲1記載の通信装置。

6．前記第1データ取得手段は、前記基準信号の自己相関関数成分と前記参照テーブルに記憶されている量子化ベクトルとを畳み込み演算し、前記遅延プロファイルと畳み込み演算した前記量子化ベクトルとを用いてメトリクス演算してベクトルコードを選択することにより前記第1データを取得することを特徴とする請求の範囲5記載の通信装置。

7．前記第1データ取得手段は、前記伝搬環境推定手段にて作成した前記遅延

プロファイルを直交変換して信号成分を凝縮した後に、当該信号成分を用いて前記第１データを取得することを特徴とする請求の範囲５記載の通信装置。

８．前記伝搬環境推定手段により得られた前記推定値に基づいて受信信号を等化処理して第２データを取得する等化手段を具備することを特徴とする請求の範囲１記載の通信装置。

９．第１通信装置は、信号を送信する際の伝搬環境を制御する伝搬環境制御手段と、前記伝搬環境制御手段にて制御した伝搬環境にて前記信号を送信する送信手段とを具備し、前記第２通信装置は、前記第１通信装置から送信された前記信号を受信して当該信号を用いて伝搬環境を推定する第１伝搬環境推定手段と、前記第１伝搬環境推定手段により得られた推定値を用いて第１データを取得する第１データ取得手段と、を具備することを特徴とする通信システム。

１０．前記第１通信装置は、前記第２通信装置から送信された信号を用いて伝搬環境を推定する第２伝搬環境推定手段と、複数のアンテナ素子とを具備し、前記送信手段は、前記第２伝搬環境推定手段により得られた推定値を用いて特定の前記第２通信装置が前記第１データを取得することができるように前記アンテナ素子毎に送信信号に重み付けして送信することを特徴とする請求の範囲９記載の通信システム。

１１．前記第２通信装置は、前記第１伝搬環境推定手段により得られた前記推定値を用いて第２データを符号化する符号化手段と、前記第２データを変調する変調手段と、前記第２データを送信する送信手段と、を具備することを特徴とする請求の範囲９記載の通信システム。

１２．通信相手から送信された信号を用いて伝搬環境を推定するステップと、推定した伝搬環境の推定値を用いて第１データを取得するステップと、を具備することを特徴とする受信方法。

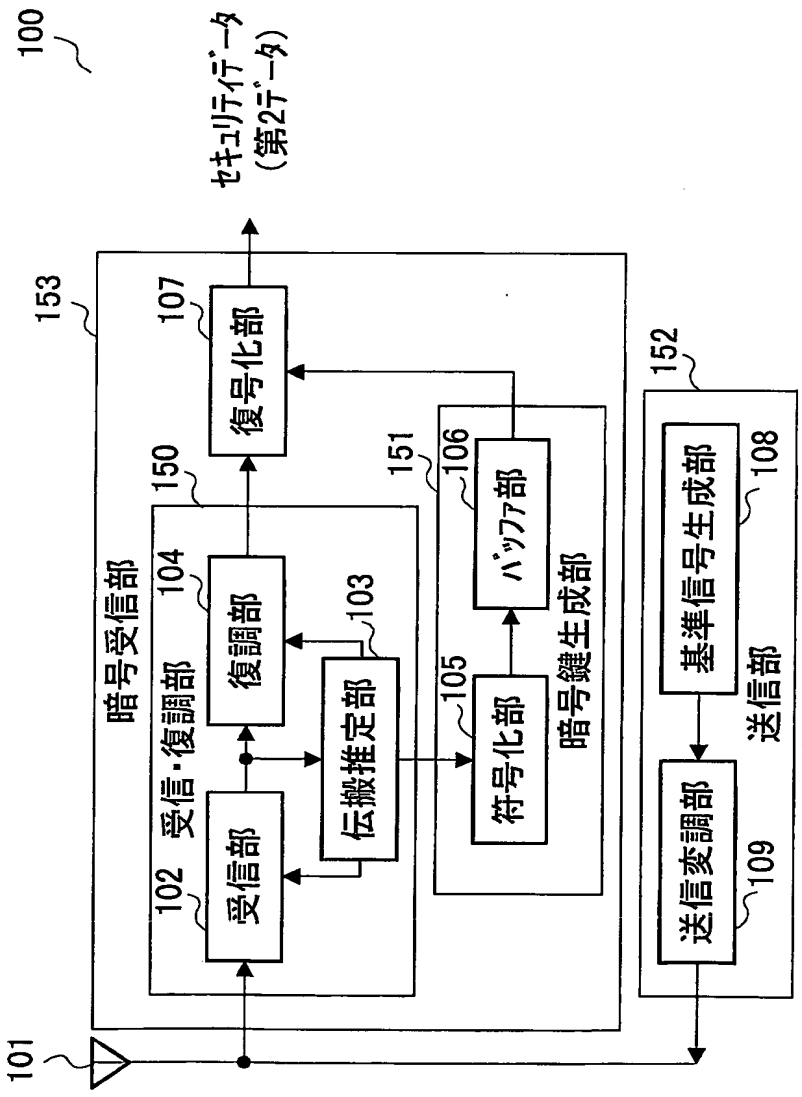

100
セキュリティデータ
(第2データ)
153
107
復号化部
暗号受信部
150
104
復調部
受信・復調部
103
伝搬推定部
102
受信部
151
106
バッファ部
105
符号化部
暗号鍵生成部
152
108
基準信号生成部
送信部
109
送信変調部
101

図1

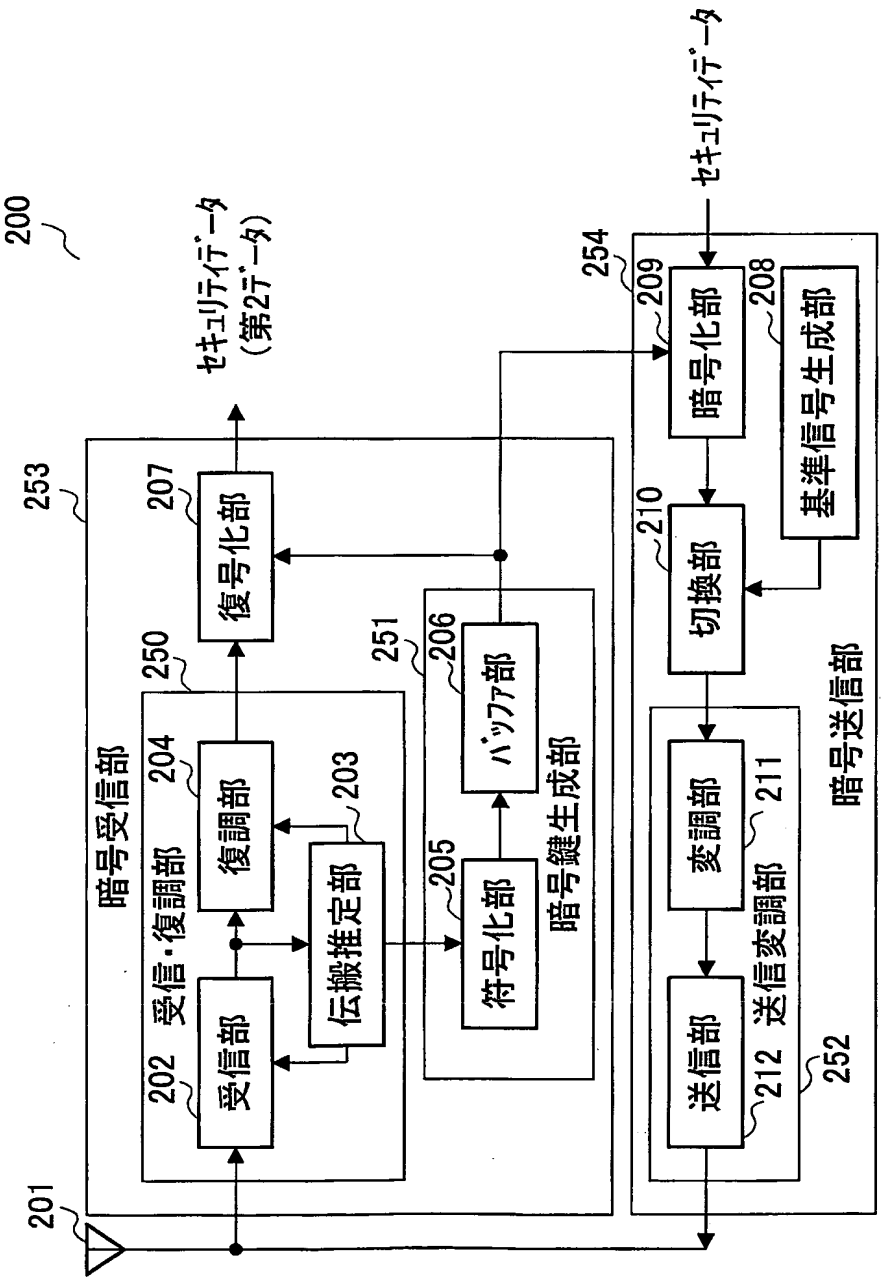

200
セキュリティデータ
(第2データ)
セキュリティデータ
253
254
207
209
208
暗号受信部
暗号化部
基準信号生成部
250
251
206
210
復号化部
バッファ部
切換部
204
203
復調部
伝搬推定部
205
211
暗号鍵生成部
変調部
暗号送信部
202
受信部
符号化部
送信部
212
252
受信・復調部
送信変調部
201

図2

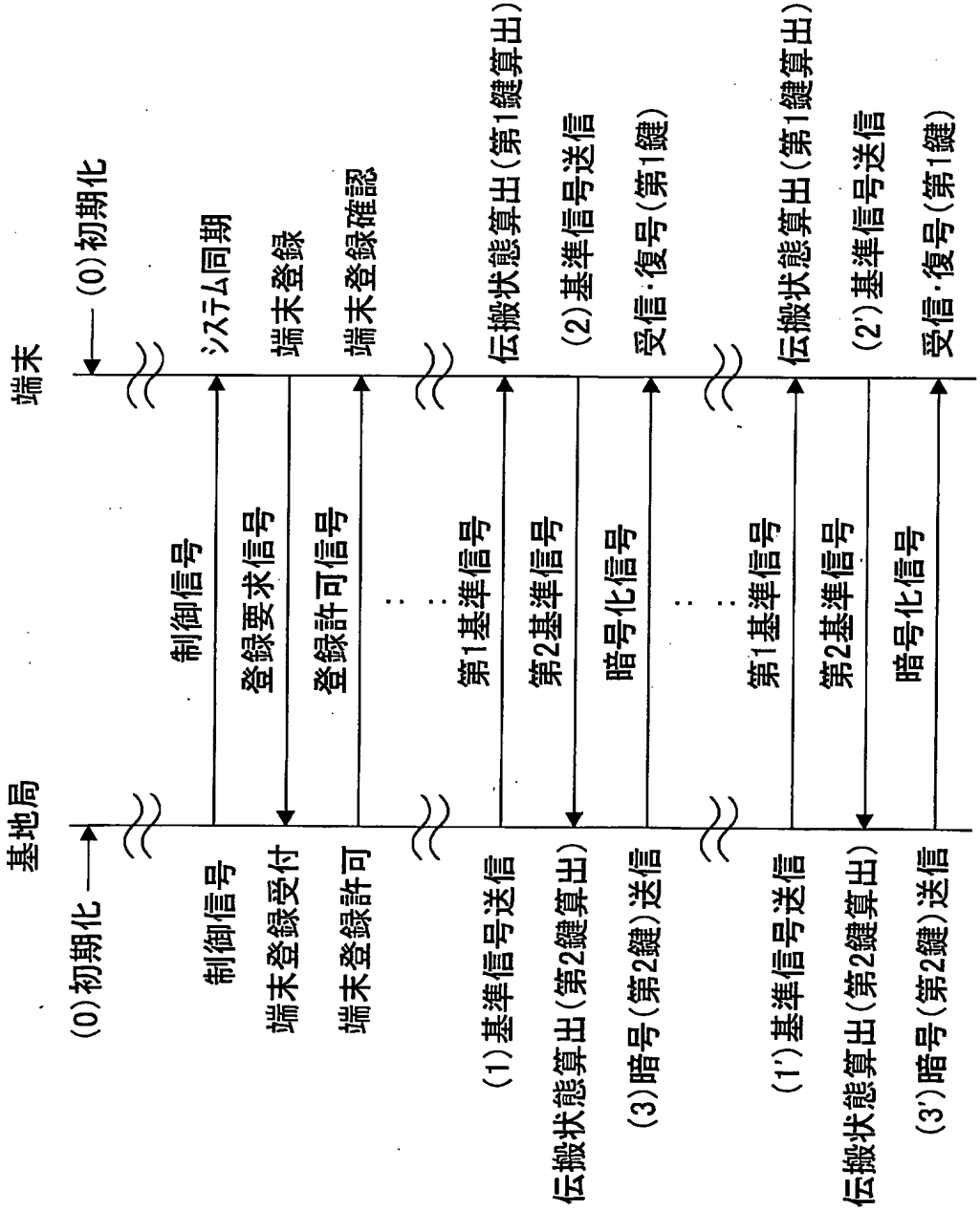

基地局
端末
(0)初期化
(0)初期化
制御信号
システム同期
制御信号
登録要求信号
端末登録受付
登録許可信号
端末登録確認
端末登録許可
第1基準信号
伝搬状態算出(第1鍵算出)
(1)基準信号送信
第2基準信号
(2)基準信号送信
伝搬状態算出(第2鍵算出)
暗号化信号
受信・復号(第1鍵)
(3)暗号(第2鍵)送信
第1基準信号
伝搬状態算出(第1鍵算出)
(1')基準信号送信
第2基準信号
(2')基準信号送信
伝搬状態算出(第2鍵算出)
暗号化信号
受信・復号(第1鍵)
(3')暗号(第2鍵)送信

図3

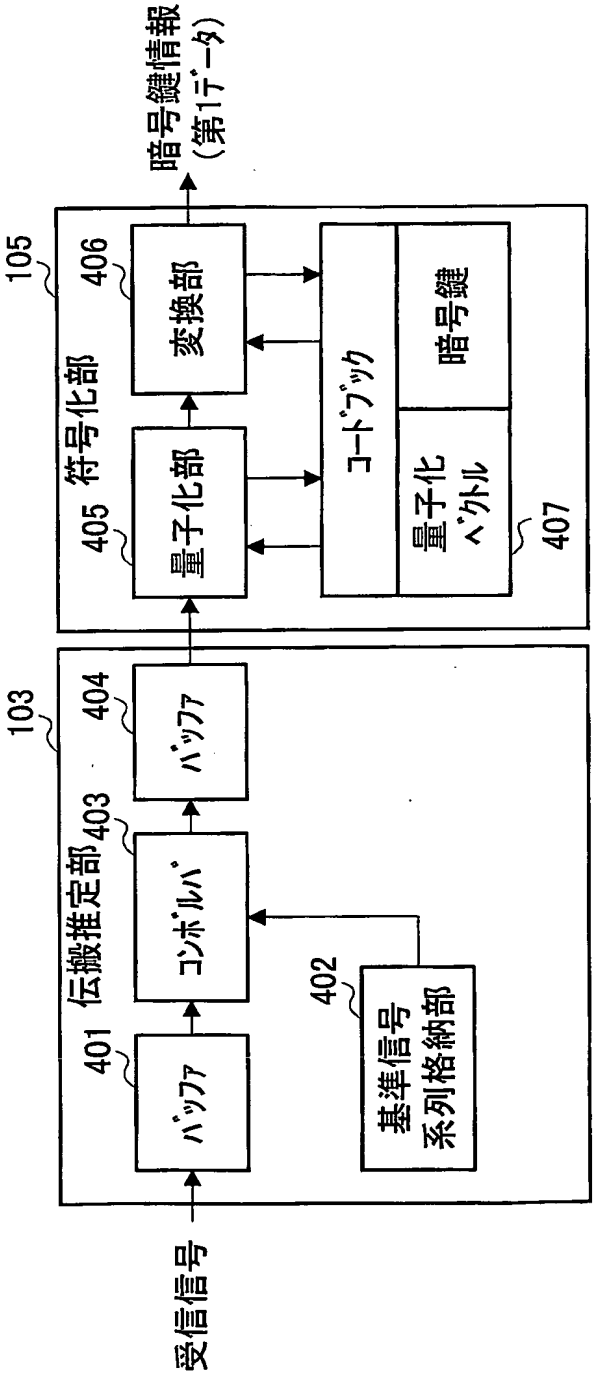

受信信号
伝搬推定部
103
401
バッファ
402
基準信号
系列格納部
403
コンボルバ
404
バッファ
符号化部
105
405
量子化部
406
変換部
コードブック
量子化
ベクトル
暗号鍵
407
暗号鍵情報
(第1データ)

図4

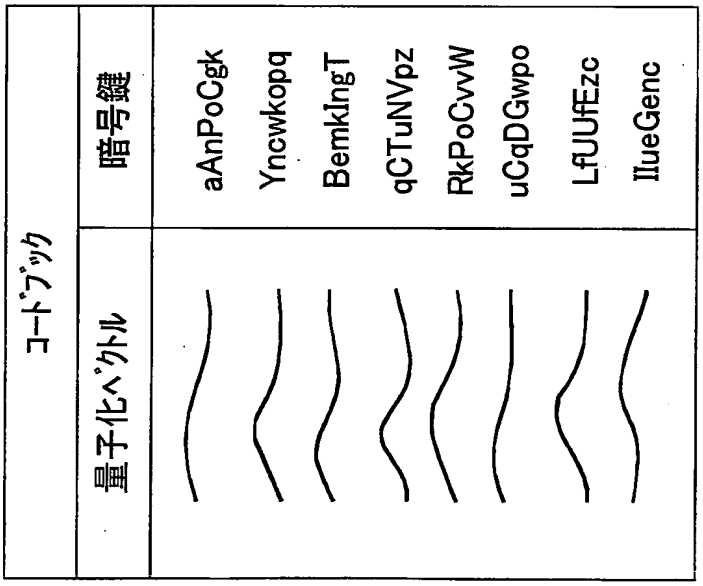

ユートピア
量子化ベクトル
暗号鍵
aAnPoCgk
Yncwkopq
BemkIngT
qCTuNVpz
RkPoCvvW
uCqDGwpo
LfUUffEzc
IlueGenc

図5

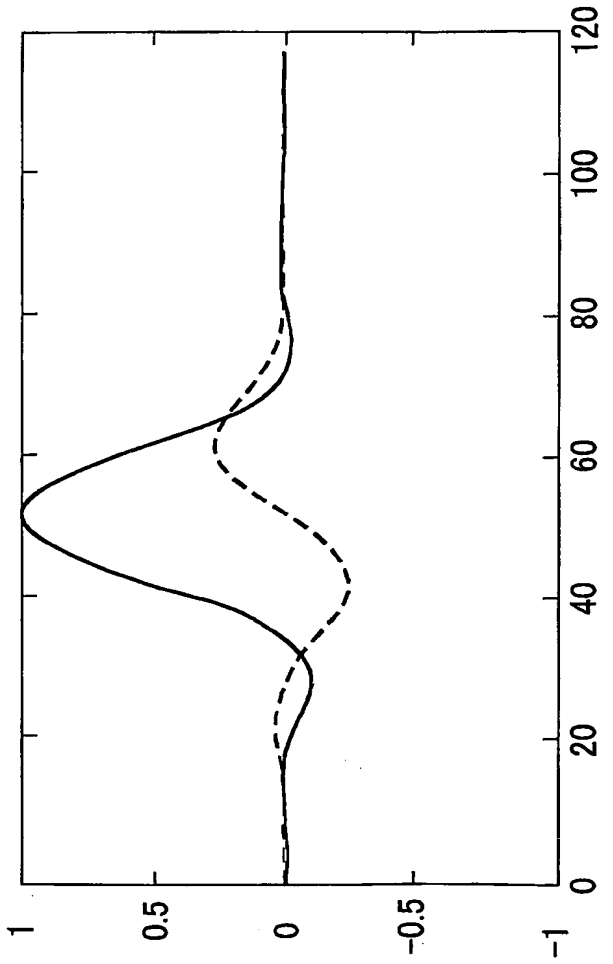


図6

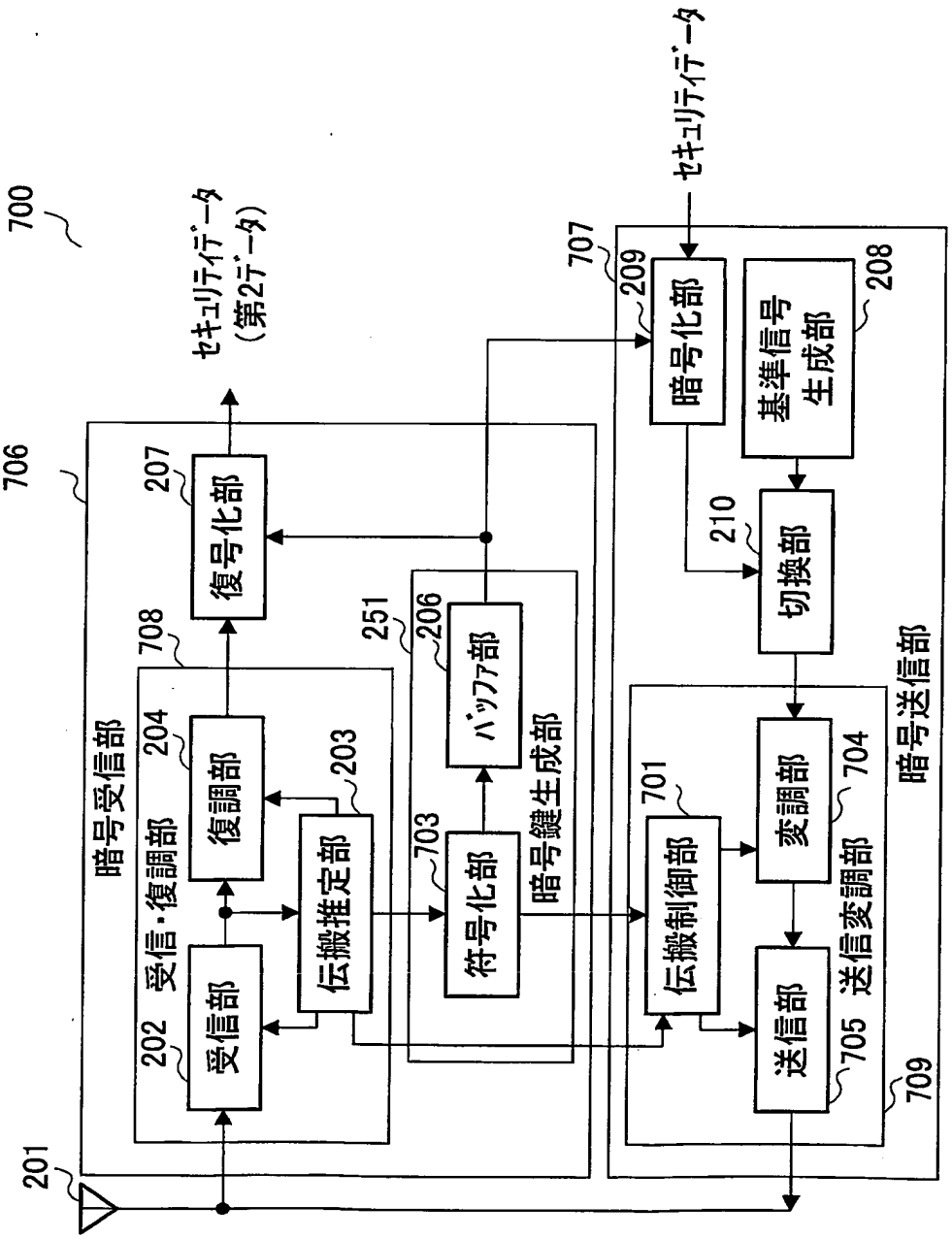

700
セキュリティデータ
(第2データ)
セキュリティデータ
706
707
207
209
208
暗号化部
基準信号
生成部
210
切換部
708
251
206
バッファ部
暗号受信部
204
203
703
701
704
復調部
伝搬推定部
符号化部
暗号鍵生成部
伝搬制御部
変調部
受信・復調部
202
受信部
送信部
705
送信変調部
709
暗号送信部
201

図7

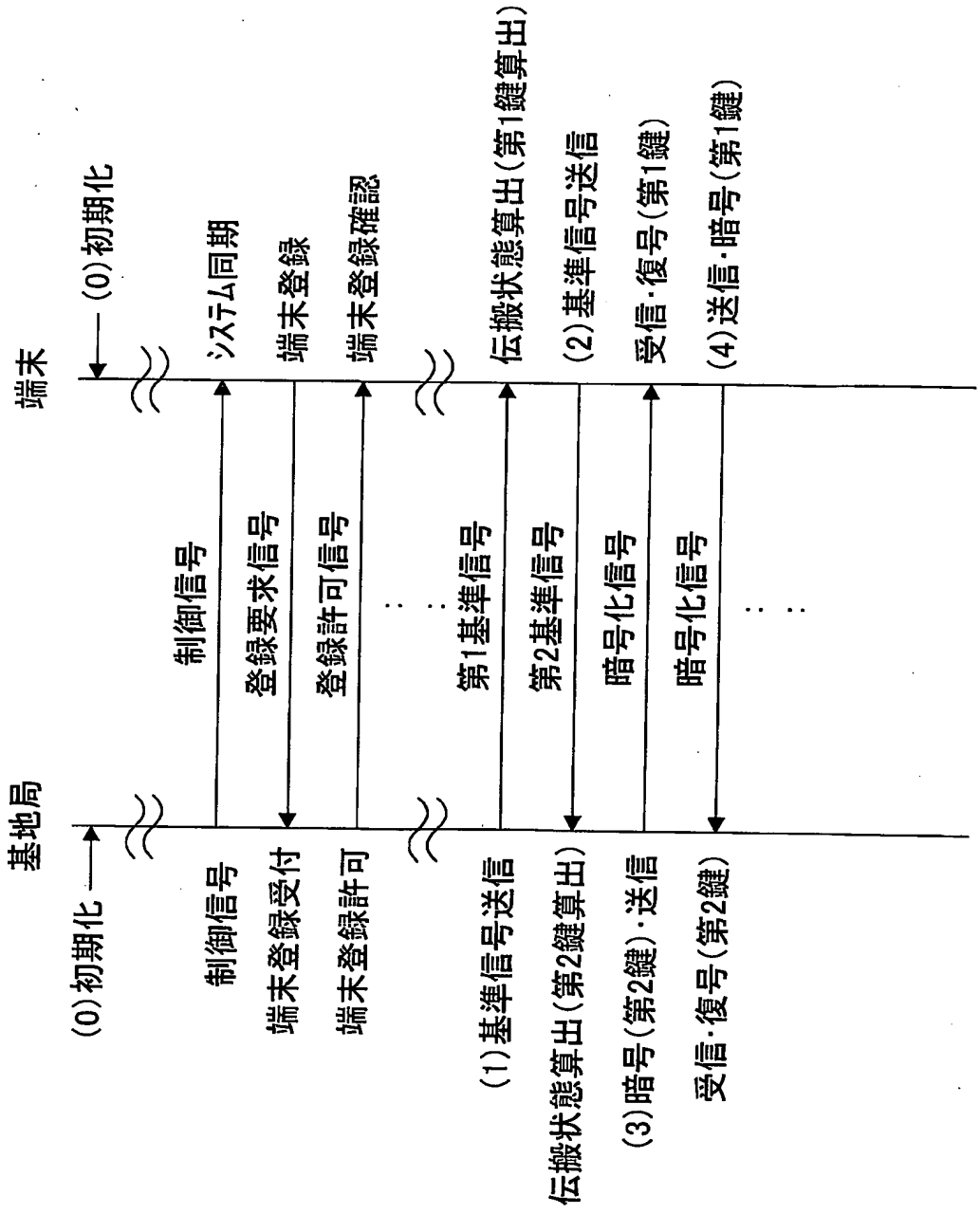

基地局
端末
(0)初期化
(0)初期化
制御信号
システム同期
制御信号
登録要求信号
端末登録
端末登録受付
登録許可信号
端末登録確認
端末登録許可
第1基準信号
(1)基準信号送信
伝搬状態算出(第1鍵算出)
第2基準信号
伝搬状態算出(第2鍵算出)
(2)基準信号送信
暗号化信号
(3)暗号(第2鍵)・送信
受信・復号(第1鍵)
暗号化信号
受信・復号(第2鍵)
(4)送信・暗号(第1鍵)

図8

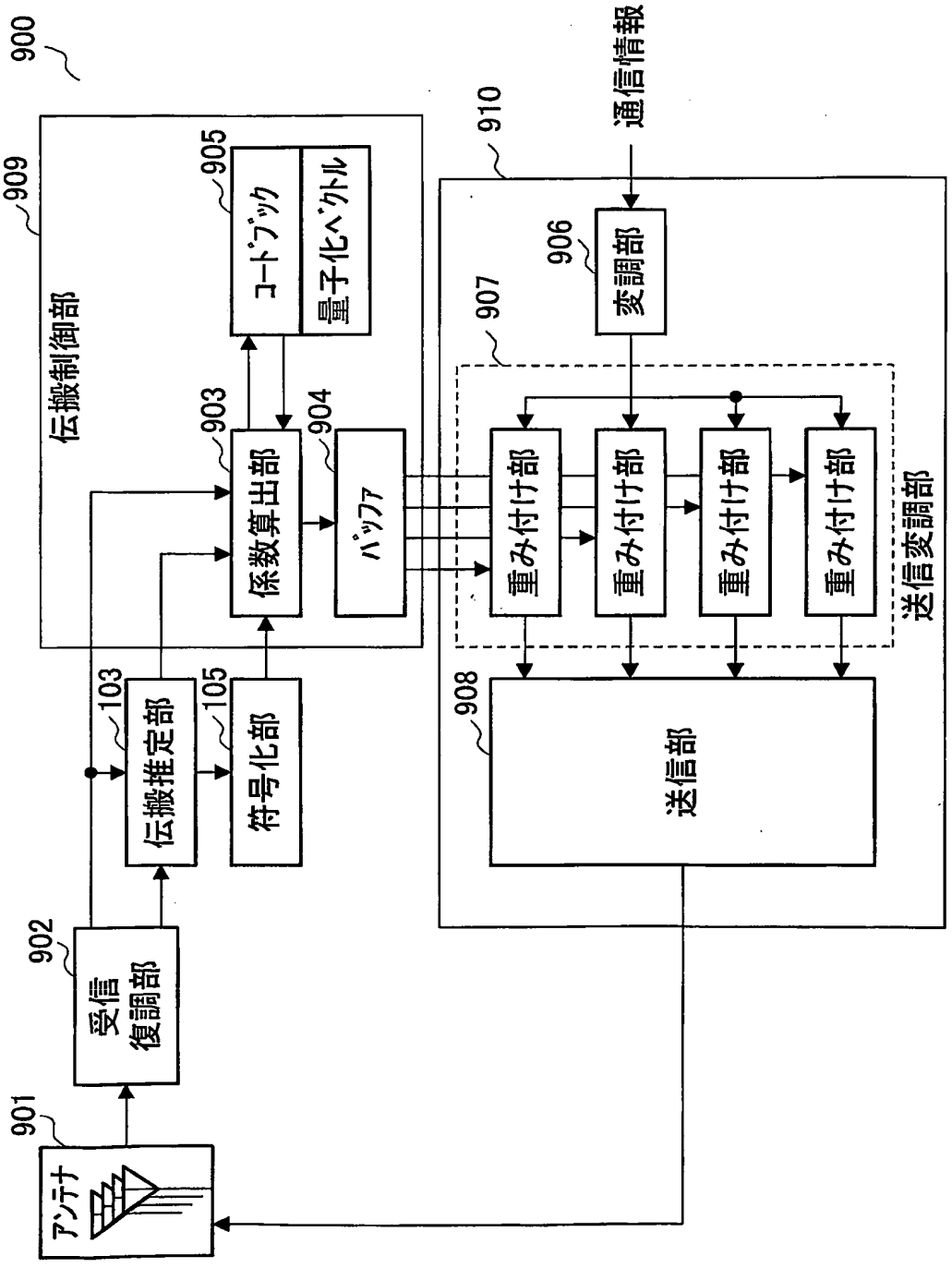

900
909
伝搬制御部
905
コードブック
量子化ベクトル
903
係数算出部
904
バッファ
103
伝搬推定部
105
符号化部
902
受信
復調部
901
アンテナ
910
通信情報
906
変調部
907
重み付け部
重み付け部
重み付け部
重み付け部
送信変調部
908
送信部

図9

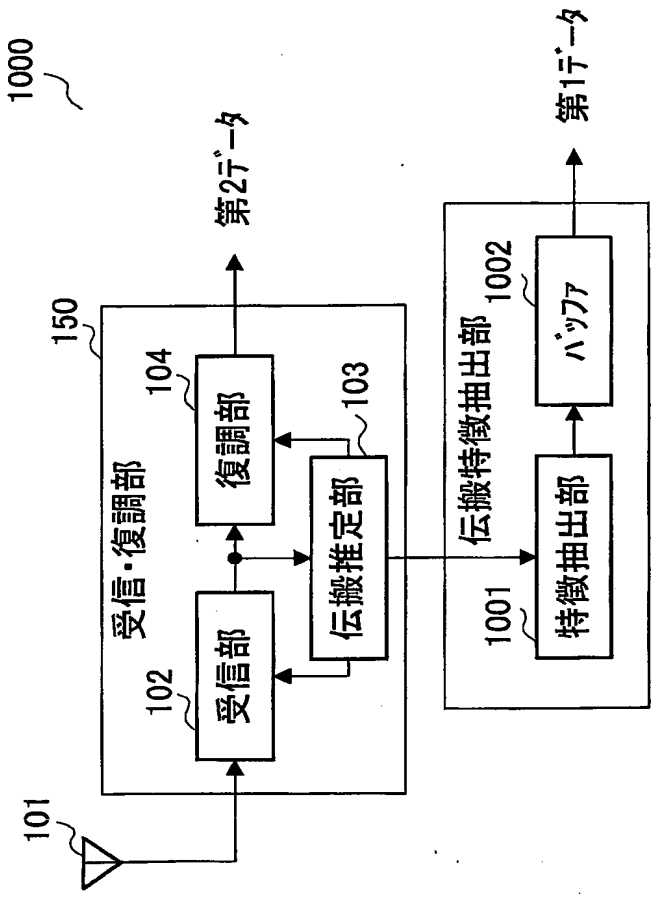

1000
第2データ
150
受信・復調部
104
復調部
103
伝搬推定部
102
受信部
101
伝搬特徴抽出部
1002
バッファ
1001
特徴抽出部
第1データ

図10

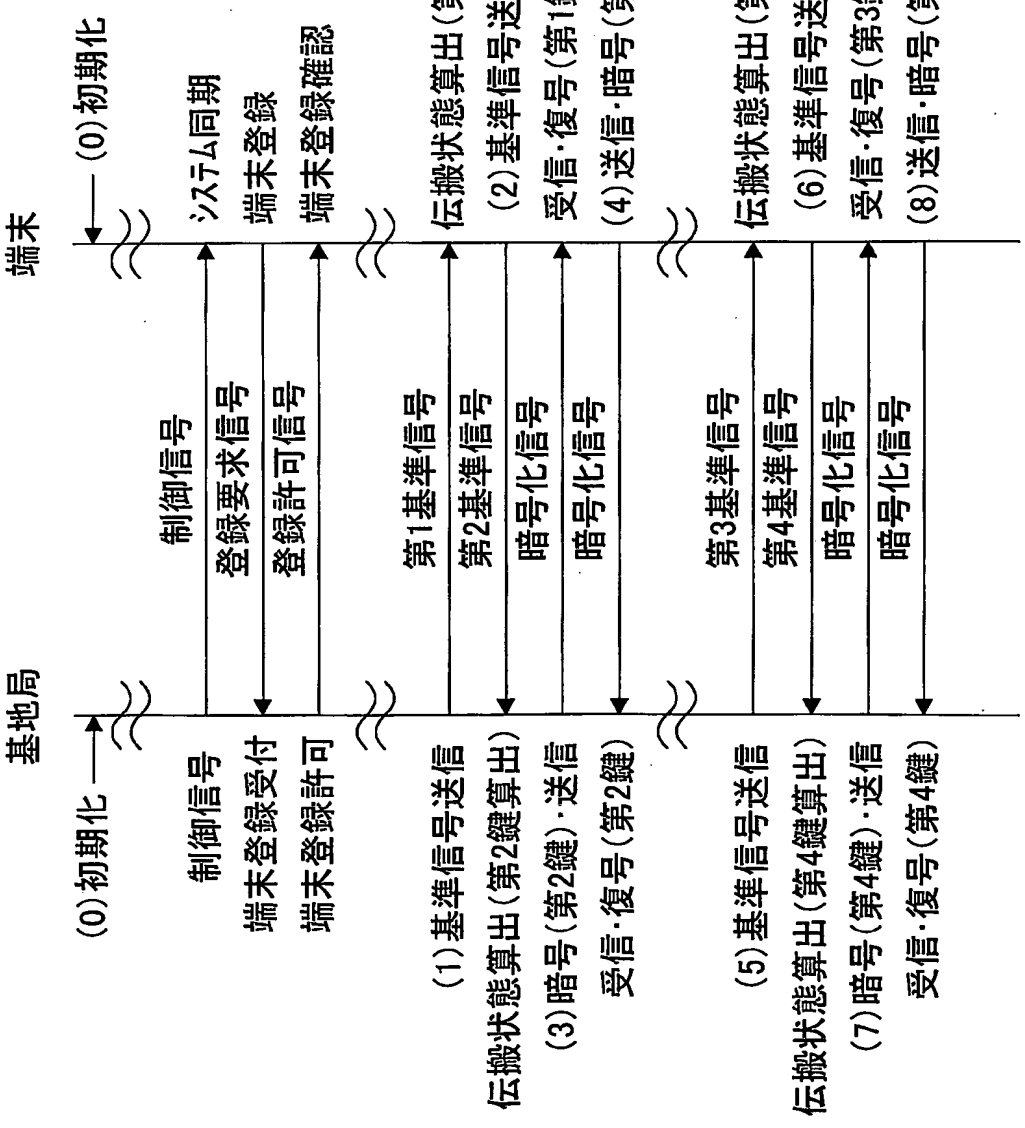

基地局
端末
(0)初期化
(0)初期化
制御信号
システム同期
登録要求信号
端末登録
登録許可信号
端末登録確認
制御信号
端末登録受付
端末登録許可
第1基準信号
伝搬状態算出(第1鍵算出)
(1)基準信号送信
第2基準信号
(2)基準信号送信
伝搬状態算出(第2鍵算出)
暗号化信号
受信・復号(第1鍵)
(3)暗号(第2鍵)・送信
暗号化信号
(4)送信・暗号(第1鍵)
受信・復号(第2鍵)
第3基準信号
伝搬状態算出(第3鍵算出)
(5)基準信号送信
第4基準信号
(6)基準信号送信
伝搬状態算出(第4鍵算出)
暗号化信号
受信・復号(第3鍵)
(7)暗号(第4鍵)・送信
暗号化信号
(8)送信・暗号(第3鍵)
受信・復号(第4鍵)

図11

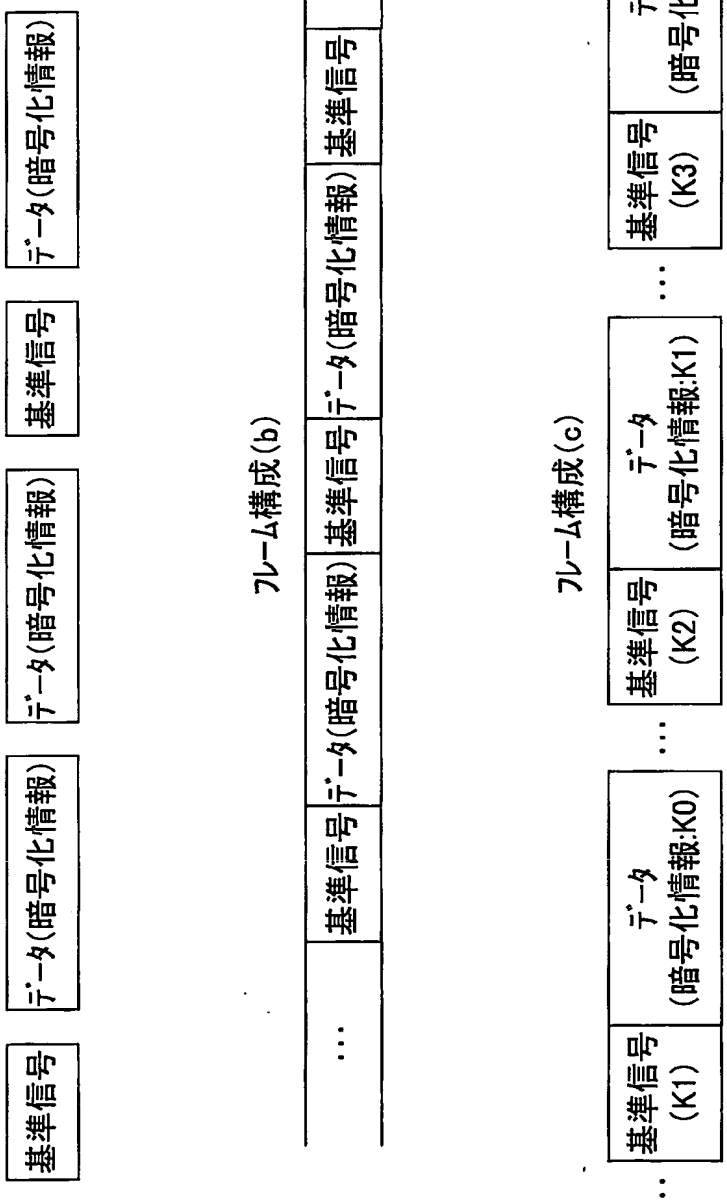

フレーム構成(a)
基準信号
データ(暗号化情報)
データ(暗号化情報)
基準信号
データ(暗号化情報)
フレーム構成(b)
…
基準信号
データ(暗号化情報)
基準信号
データ(暗号化情報)
基準信号
…
フレーム構成(c)
…
基準信号 (K1)
データ (暗号化情報:K0)
…
基準信号 (K2)
データ (暗号化情報:K1)
…
基準信号 (K3)
データ (暗号化情報:K2)
…

図12

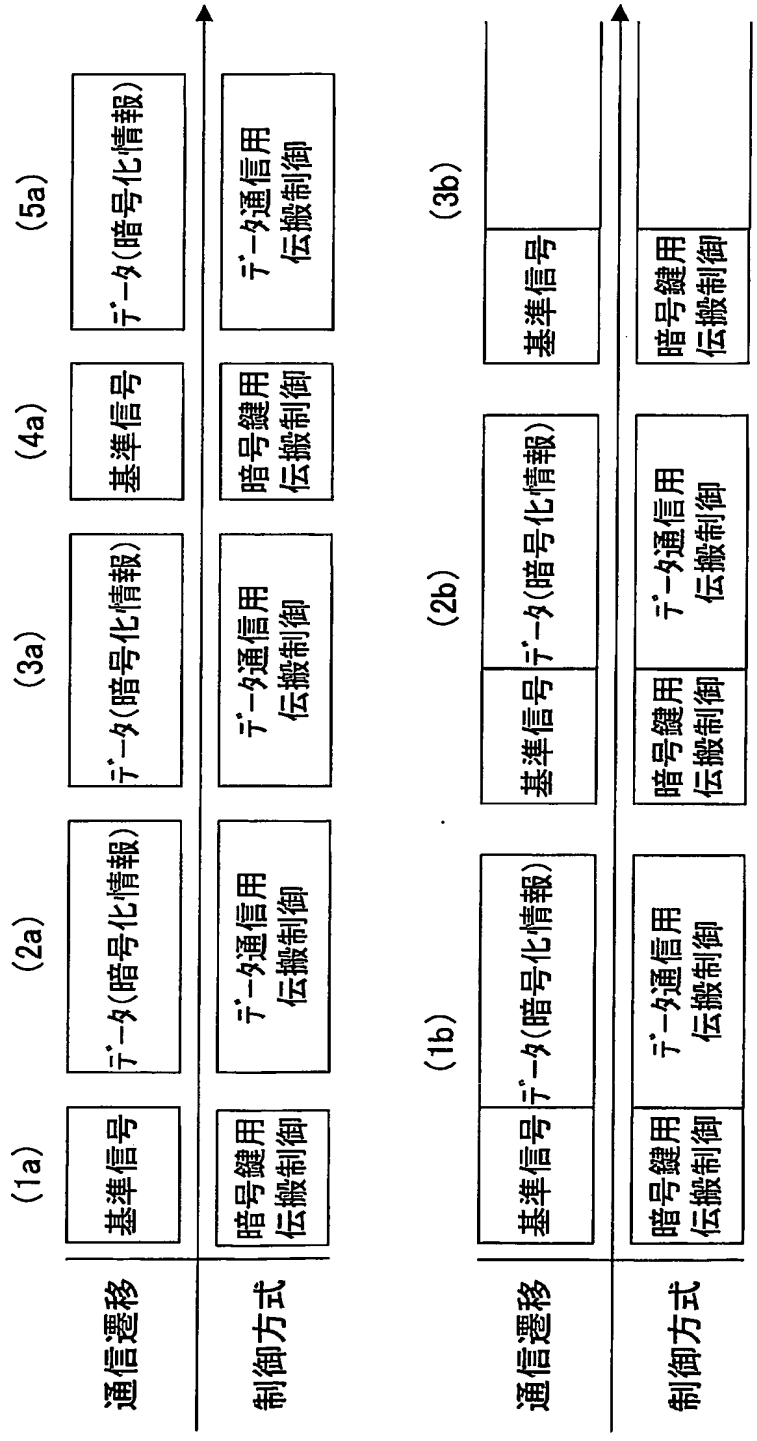

(1a)
(2a)
(3a)
(4a)
(5a)
通信遷移
基準信号
データ(暗号化情報)
データ(暗号化情報)
基準信号
データ(暗号化情報)
制御方式
暗号鍵用伝搬制御
データ通信用伝搬制御
データ通信用伝搬制御
暗号鍵用伝搬制御
データ通信用伝搬制御
(1b)
(2b)
(3b)
通信遷移
基準信号
データ(暗号化情報)
基準信号
データ(暗号化情報)
基準信号
制御方式
暗号鍵用伝搬制御
データ通信用伝搬制御
暗号鍵用伝搬制御
データ通信用伝搬制御
暗号鍵用伝搬制御

図13

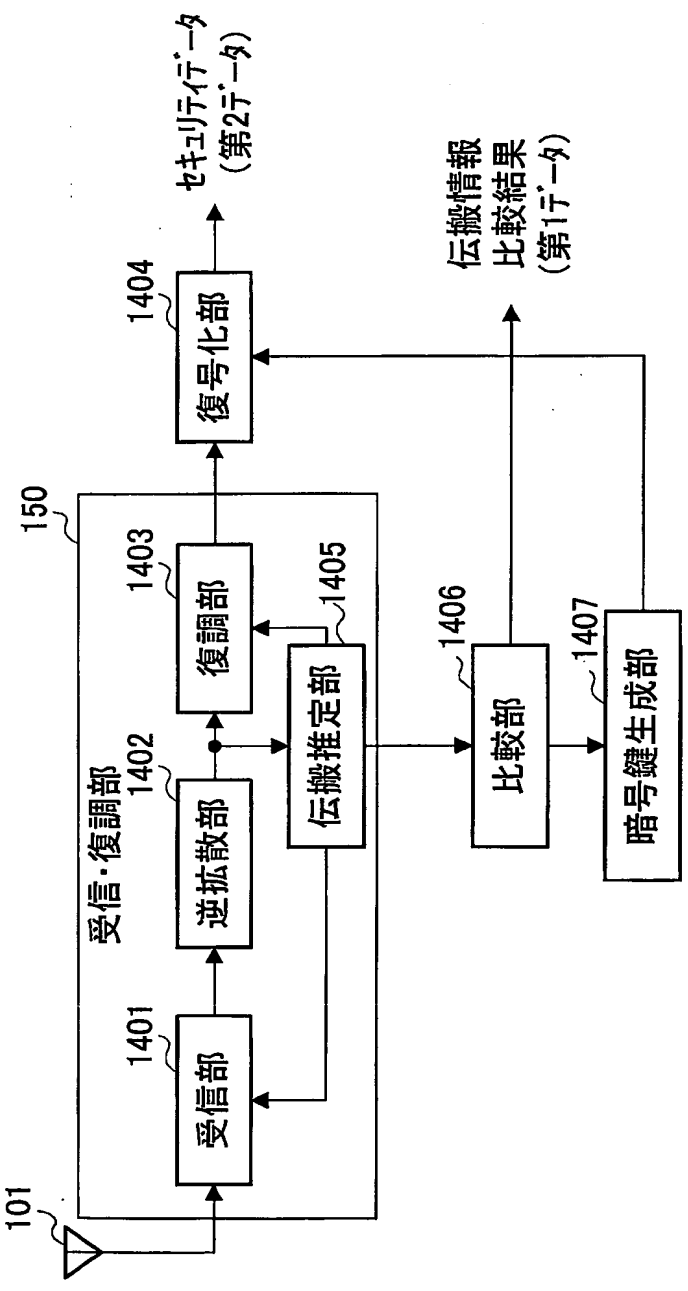

101
150
受信・復調部
1401
受信部
1402
逆拡散部
1403
復調部
1404
復号化部
1405
伝搬推定部
1406
比較部
1407
暗号鍵生成部
セキュリティデータ
(第2データ)
伝搬情報
比較結果
(第1データ)

図14

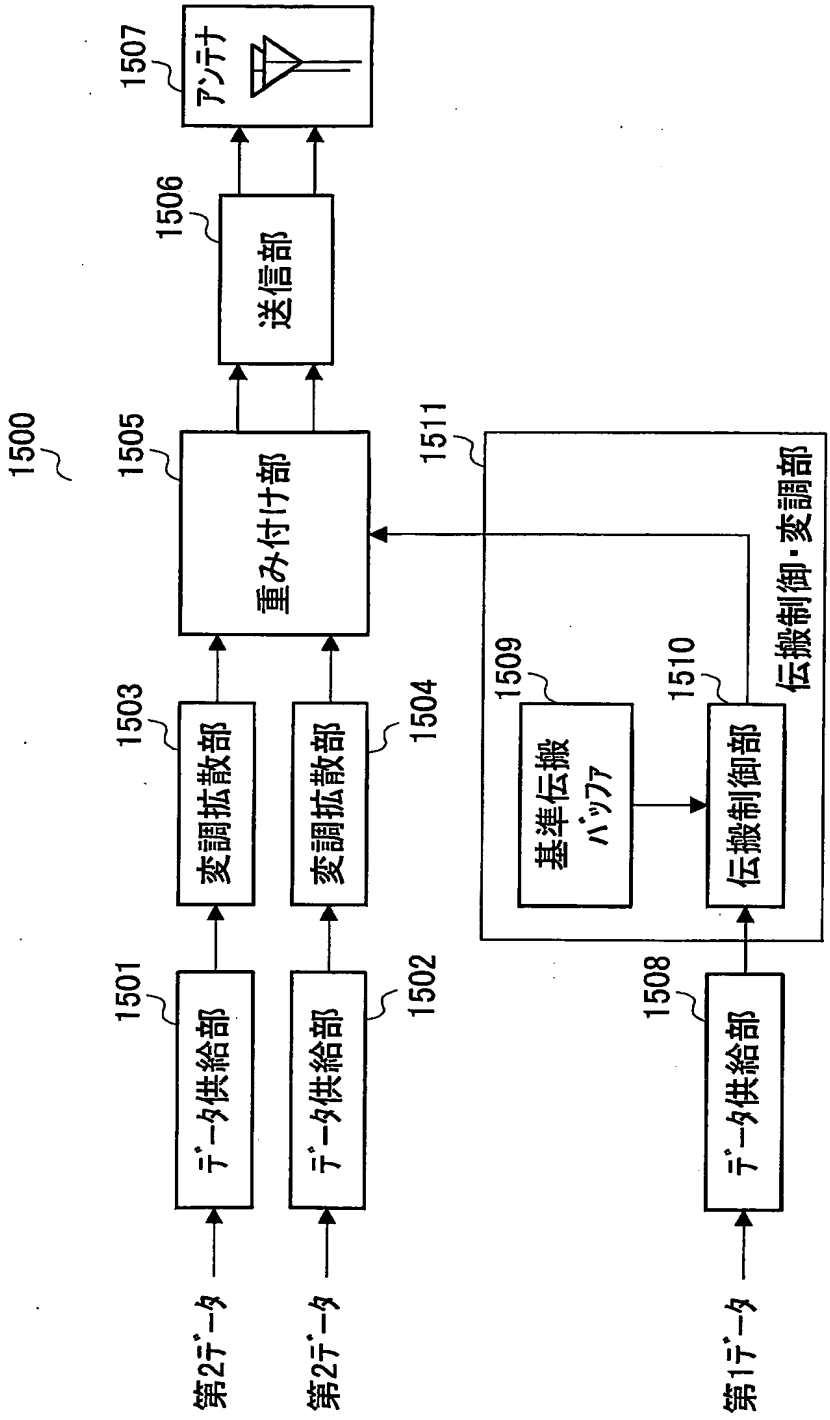

1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
第2データ
第2データ
第1データ
データ供給部
データ供給部
データ供給部
変調拡散部
変調拡散部
重み付け部
送信部
アンテナ
基準伝搬パス7
伝搬制御部
伝搬制御・変調部

図15

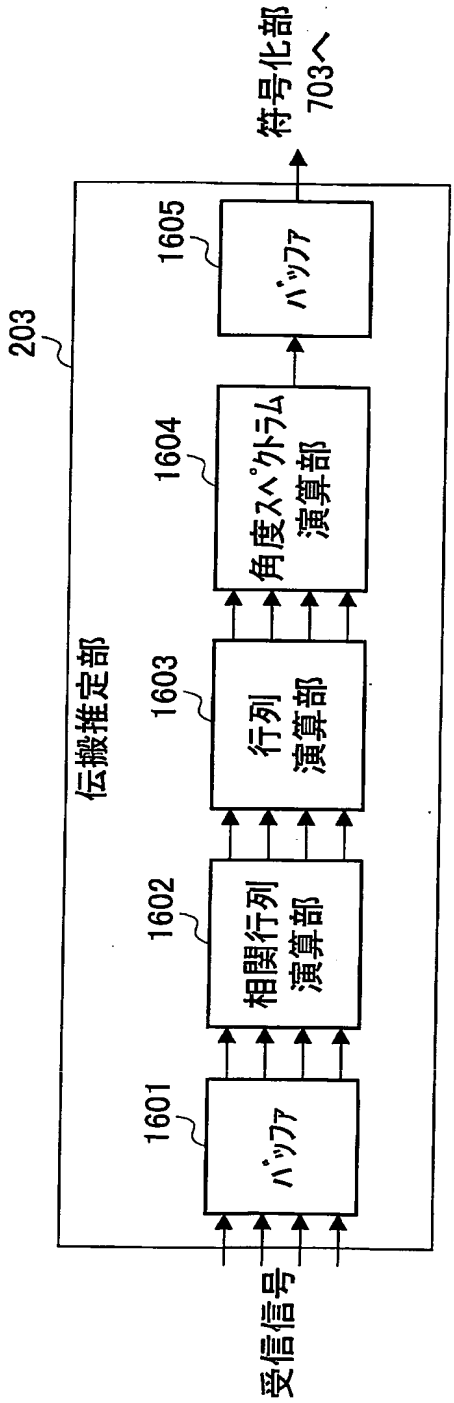

符号化部
703へ
203
伝搬推定部
1605
バッファ
1604
角度スペクトラム
演算部
1603
行列
演算部
1602
相関行列
演算部
1601
バッファ
受信信号

図16

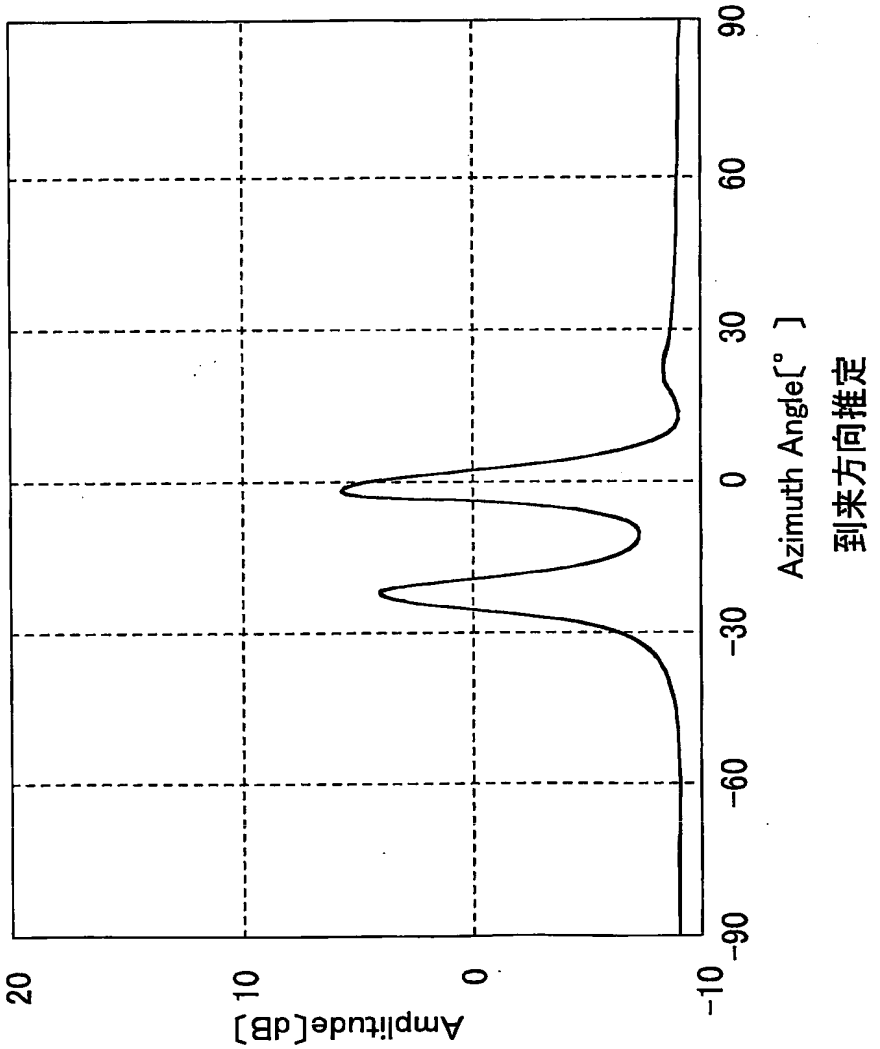


図17

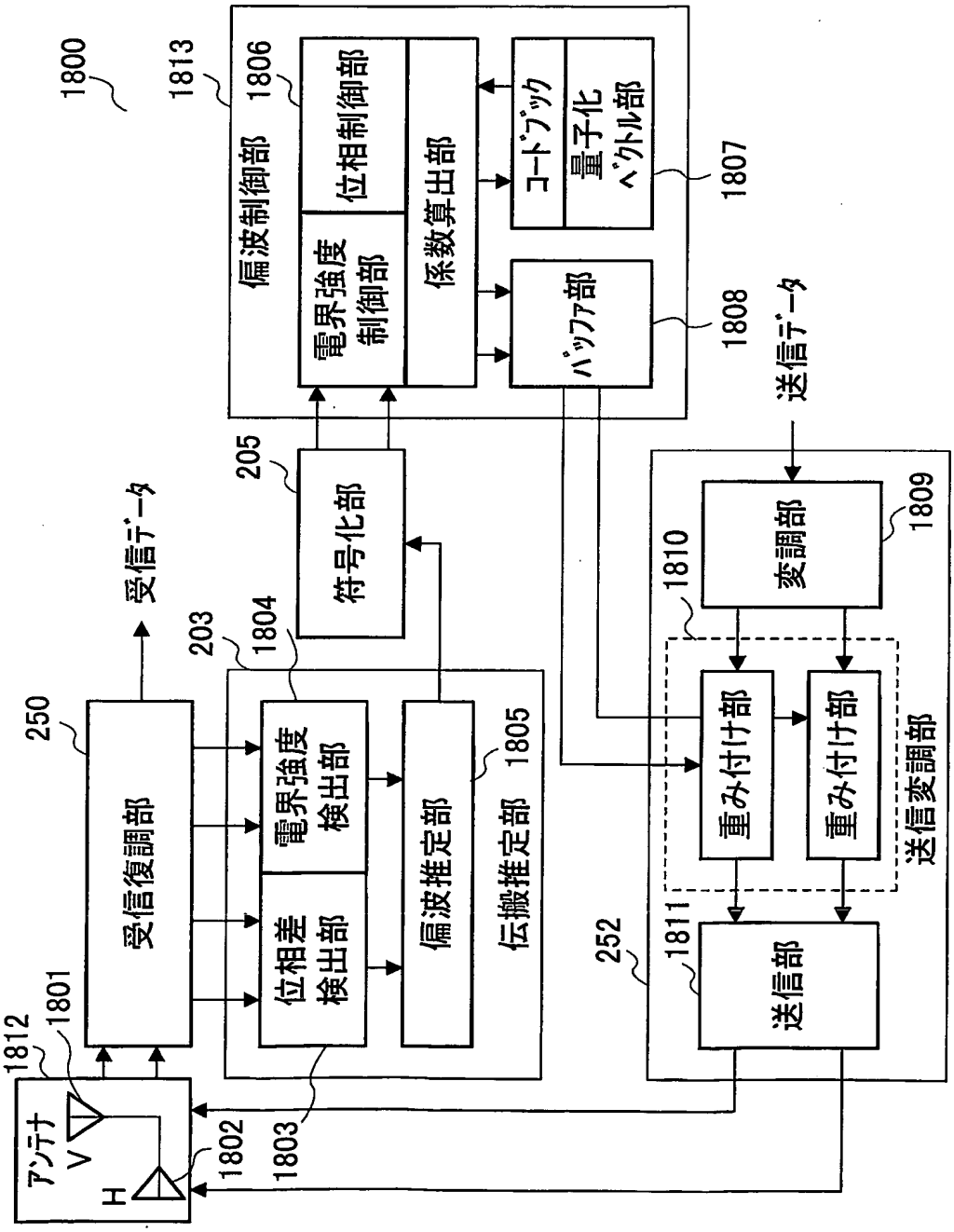

1800
1813
1806
偏波制御部
位相制御部
電界強度
制御部
係数算出部
コードブック
量子化
ベクトル部
1807
バッファ部
1808
送信データ
205
符号化部
受信データ
203
1804
250
受信復調部
電界強度
検出部
位相差
検出部
偏波推定部
1805
伝搬推定部
1810
変調部
1809
重み付け部
重み付け部
送信変調部
252
1811
送信部
1812
1801
アンテナ
V
H
1802
1803

図18

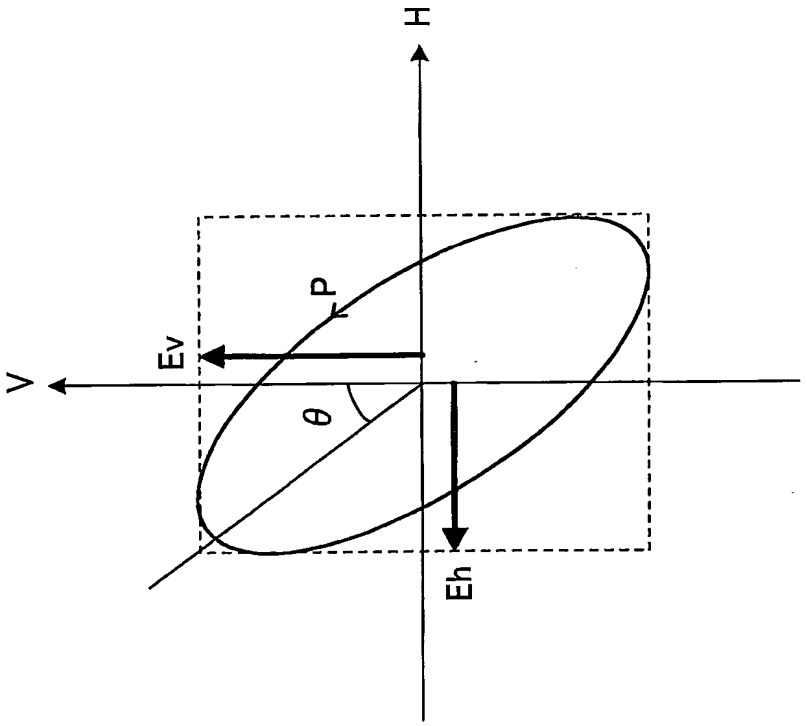


図19

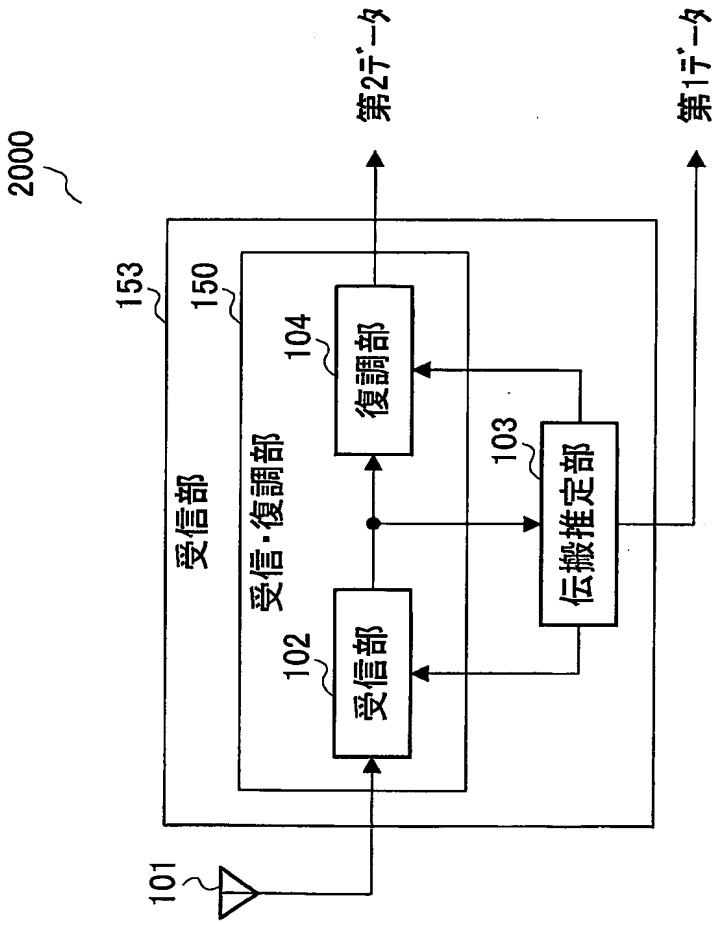

2000
第2データ
第1データ
153
150
104
復調部
103
伝搬推定部
受信部
受信・復調部
102
受信部
101

図20

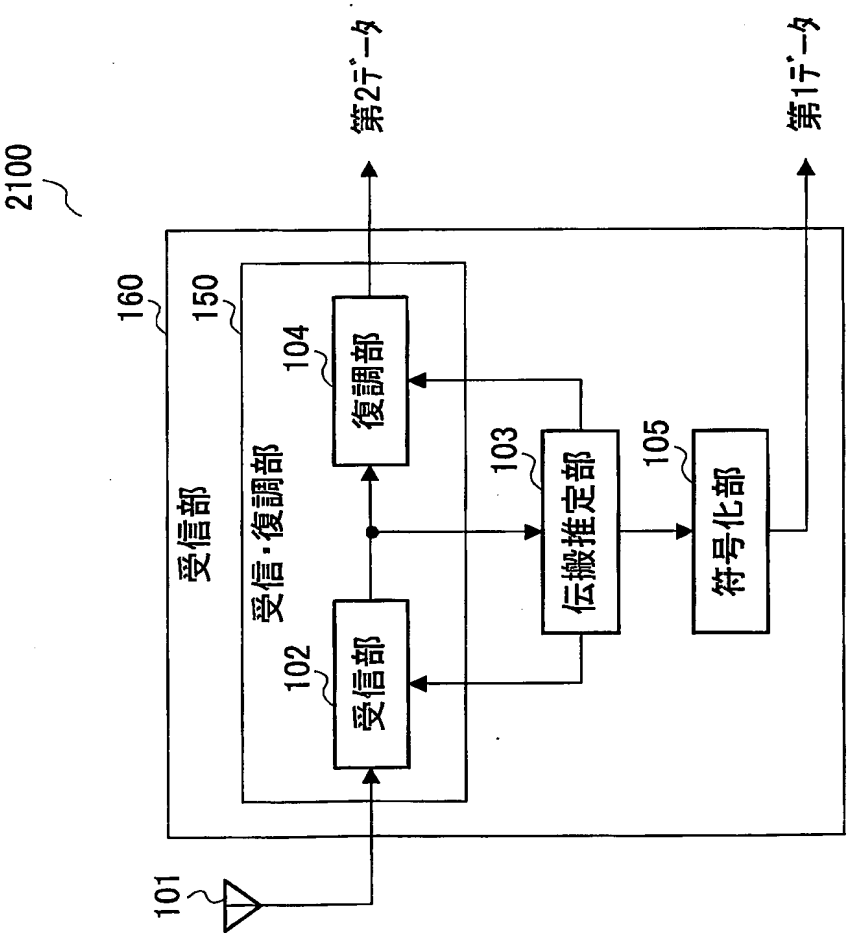

2100
第2データ
第1データ
160
150
104
復調部
受信部
受信・復調部
103
伝搬推定部
105
符号化部
102
受信部
101

図21

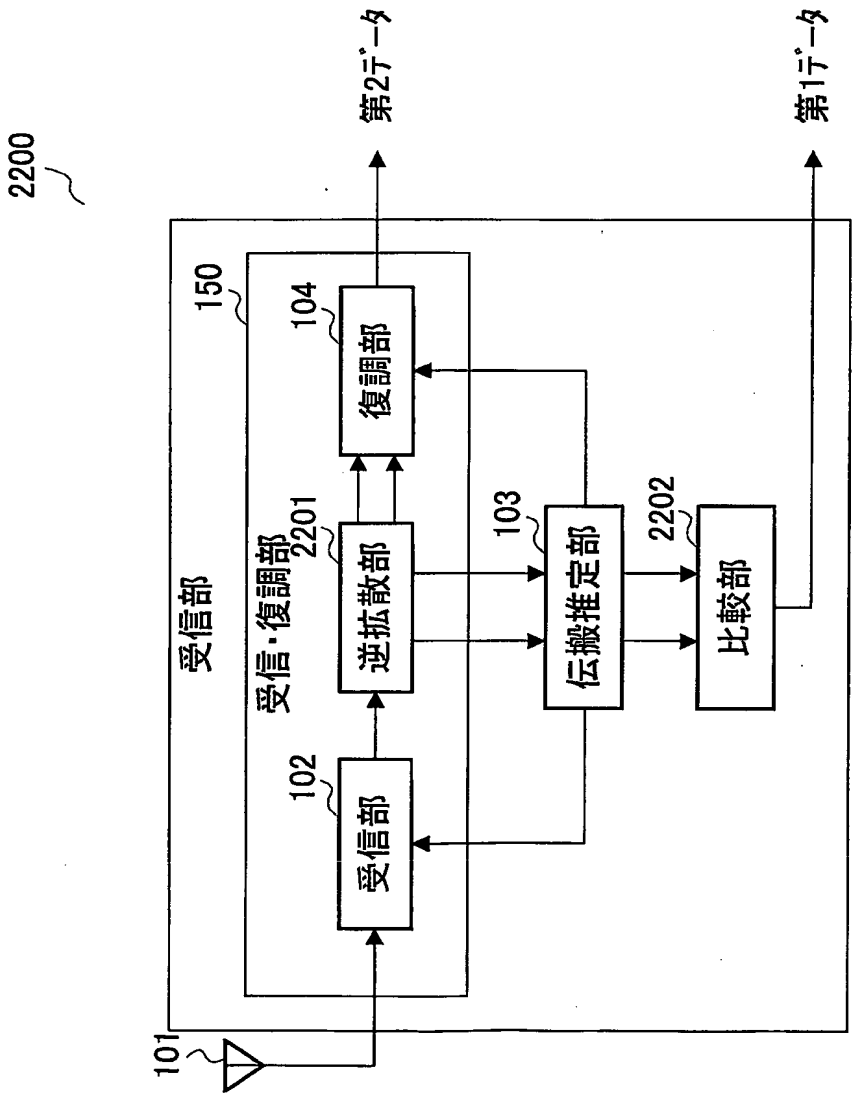

2200
第2データ
第1データ
150
104
復調部
受信・復調部
2201
逆拡散部
103
伝搬推定部
2202
比較部
受信部
102
受信部
101

図22

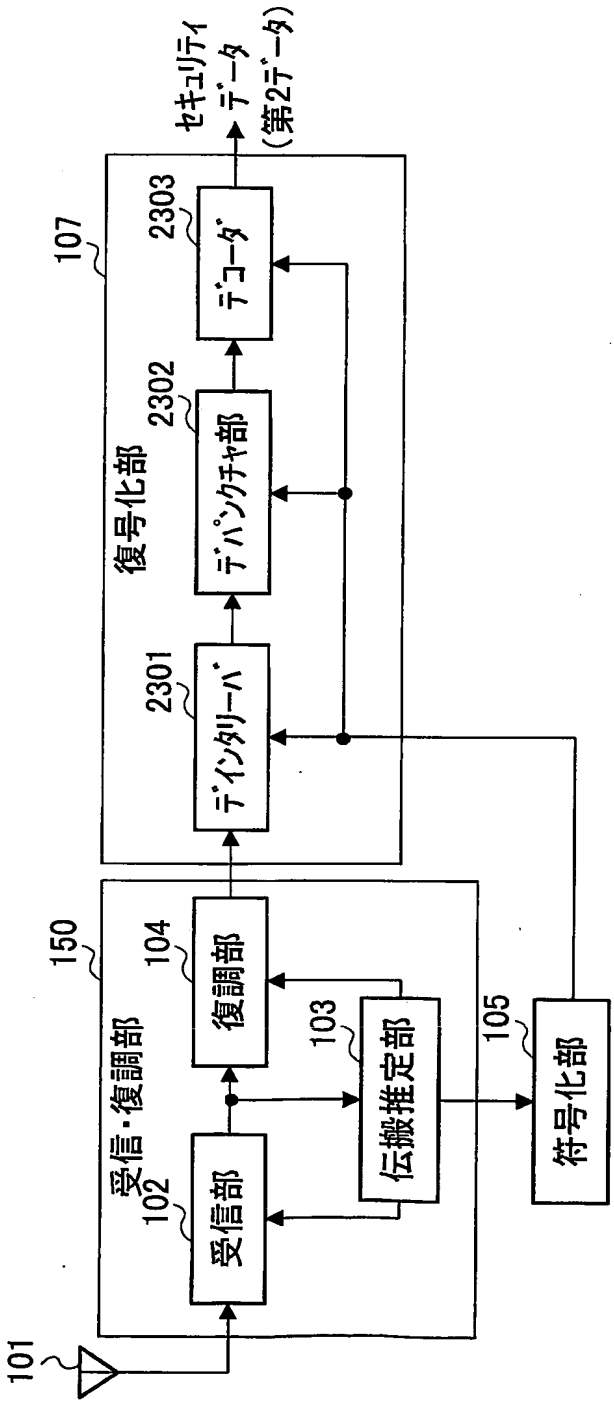

2300
101
150
受信・復調部
102
受信部
104
復調部
103
伝搬推定部
105
符号化部
107
復号化部
2301
デインタリーバ
2302
デパンクチャ部
2303
デコーダ
セキュリティデータ
(第2データ)

図23

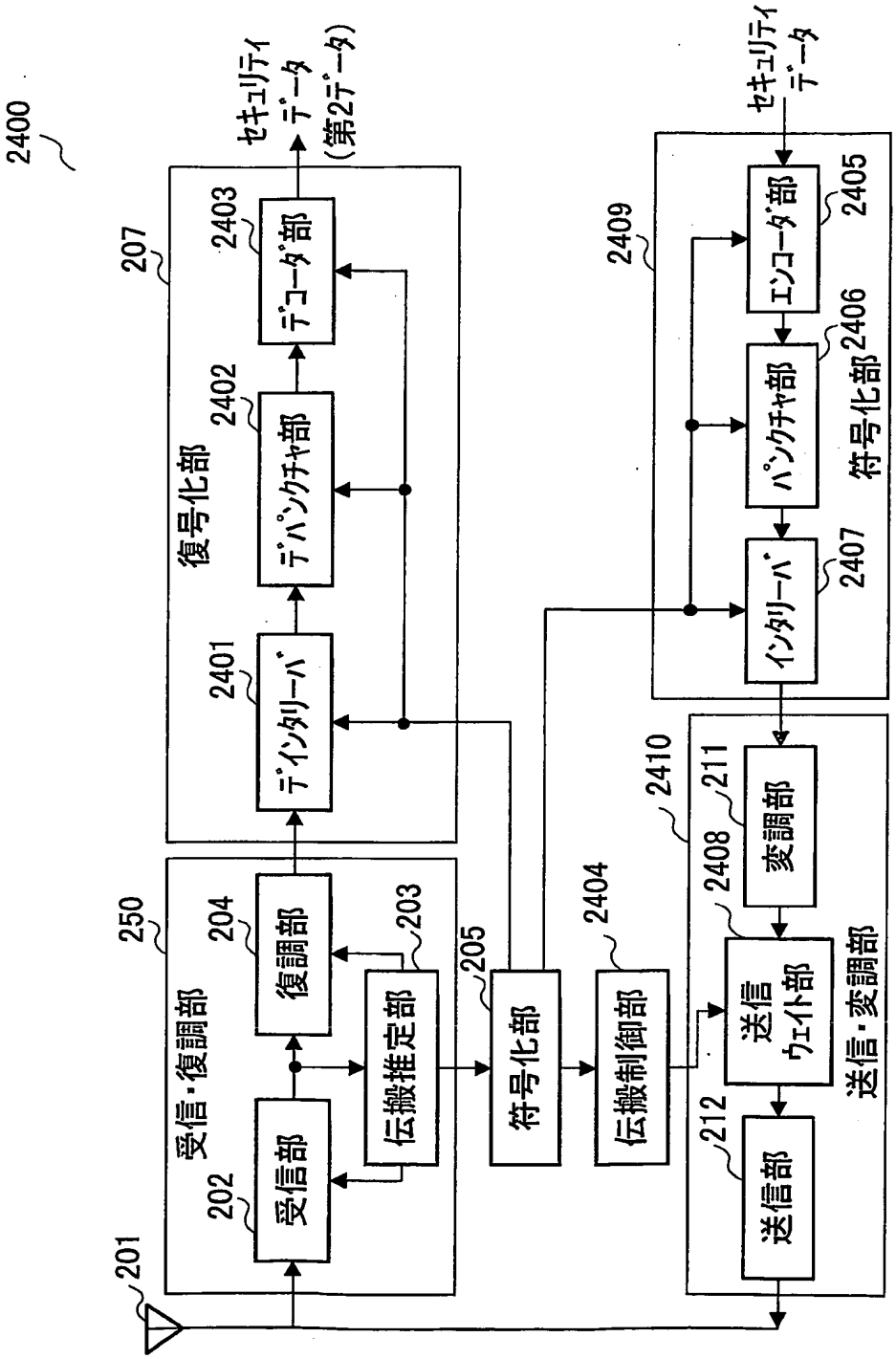

2400
セキュリティデータ (第2データ)
207
2403
デコーダ部
2402
デパンクチャ部
復号化部
2401
デインタリーバ
250
受信・復調部
204
復調部
203
伝搬推定部
202
受信部
201
205
符号化部
2404
伝搬制御部
2409
セキュリティデータ
2405
エンコーダ部
2406
パンクチャ部
符号化部
2407
インタリーバ
2410
211
変調部
2408
送信ウェイト部
212
送信部
送信・変調部

図24

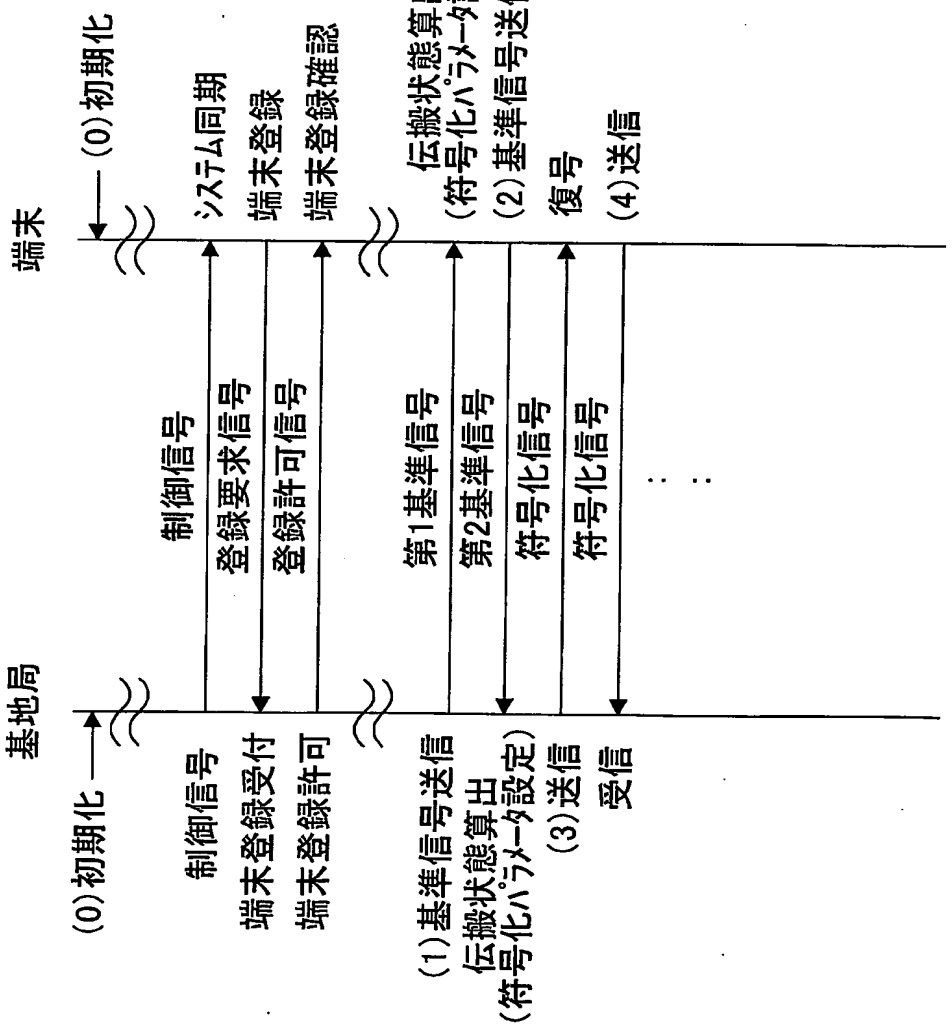

端末
基地局
(0)初期化
(0)初期化
制御信号
システム同期
登録要求信号
端末登録
登録許可信号
端末登録確認
制御信号
端末登録受付
端末登録許可
第1基準信号
伝搬状態算出
(符号化パラメータ設定)
第2基準信号
(2)基準信号送信
符号化信号
復号
符号化信号
(4)送信
(1)基準信号送信
伝搬状態算出
(符号化パラメータ設定)
(3)送信
受信

図25

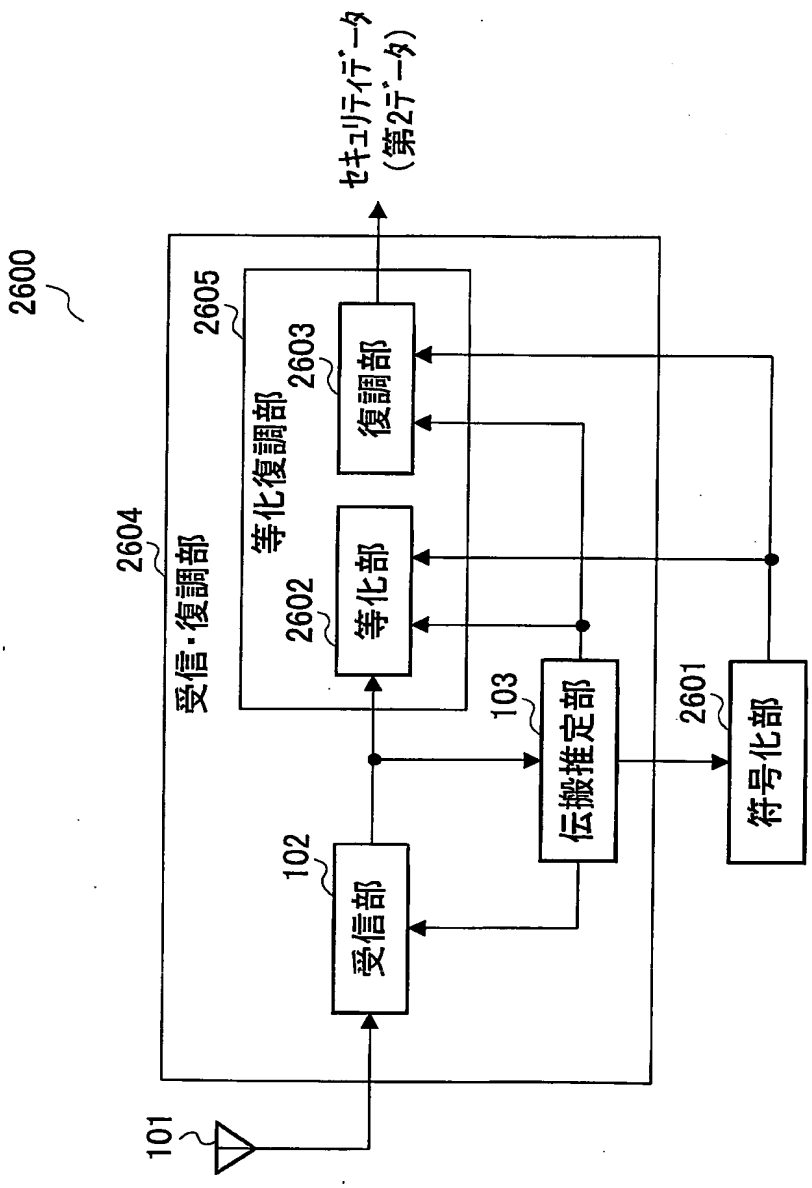

セキュリティデータ
(第2データ)
2600
2605
2603
復調部
等化復調部
2604
2602
等化部
受信・復調部
103
伝搬推定部
2601
符号化部
102
受信部
101

図26

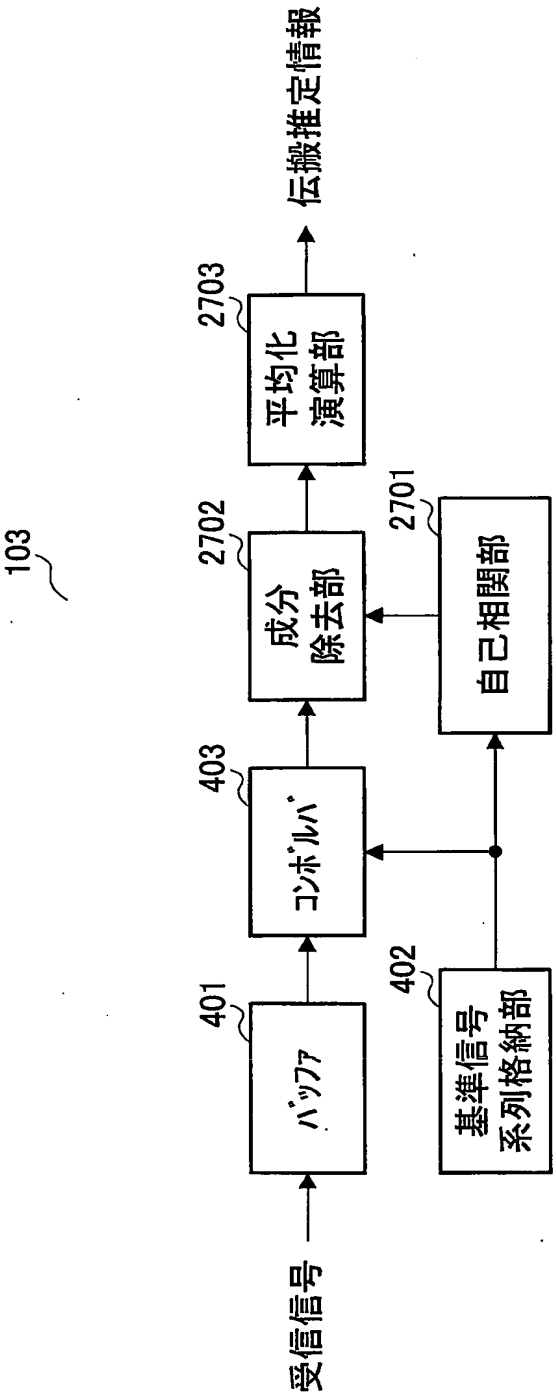

103
受信信号
401
バッファ
403
コンボルバ
402
基準信号
系列格納部
2701
自己相関部
2702
成分
除去部
2703
平均化
演算部
伝搬推定情報

図27

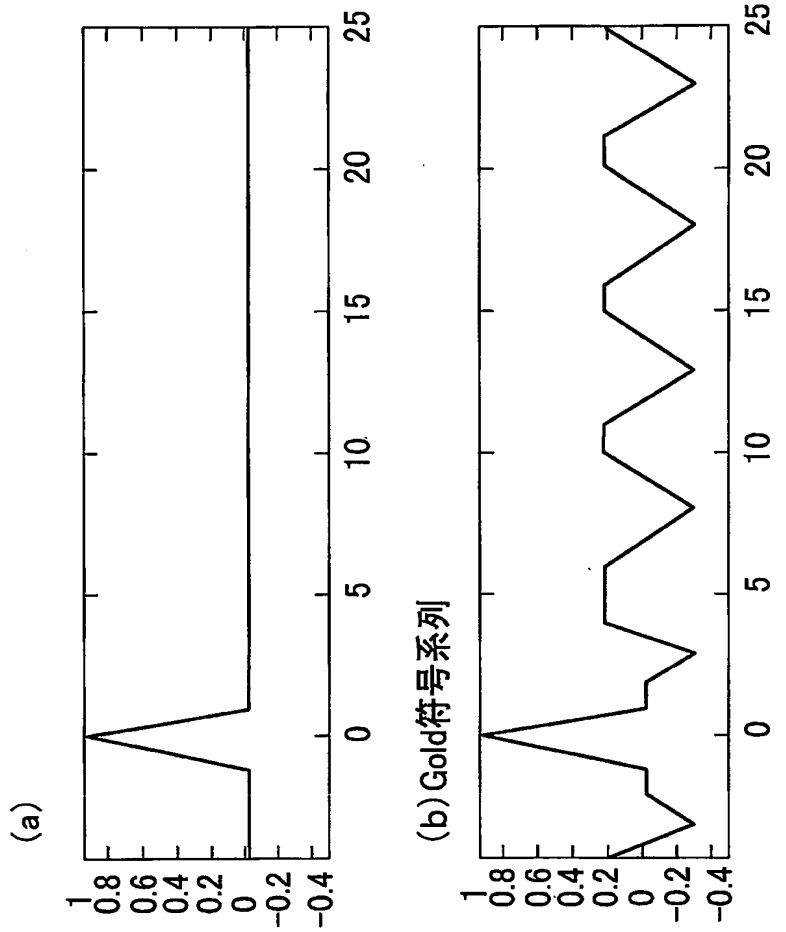

(a)
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
0
5
10
15
20
25
(b) Gold符号系列
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
0
5
10
15
20
25

図28

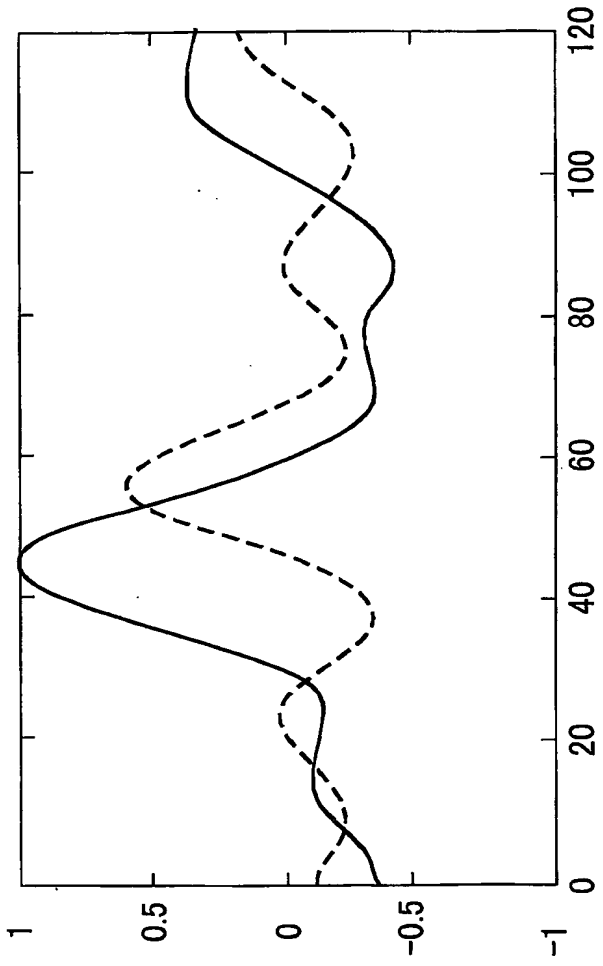


図29

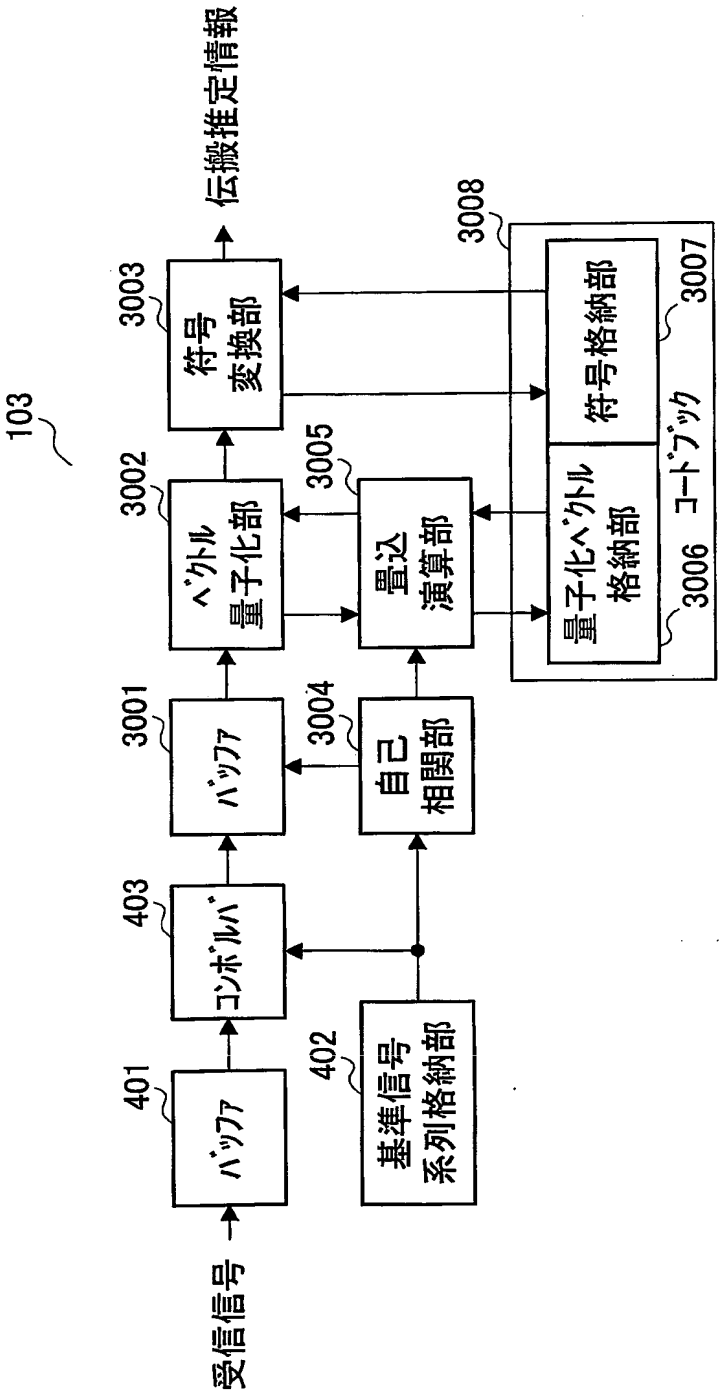

103
受信信号
401
バッファ
402
基準信号
系列格納部
403
コンボルバ
3001
バッファ
3004
自己
相関部
3002
ベクトル
量子化部
3005
畳込
演算部
3003
符号
変換部
伝搬推定情報
3008
3007
符号格納部
コードブック
3006
量子化ベクトル
格納部

図30

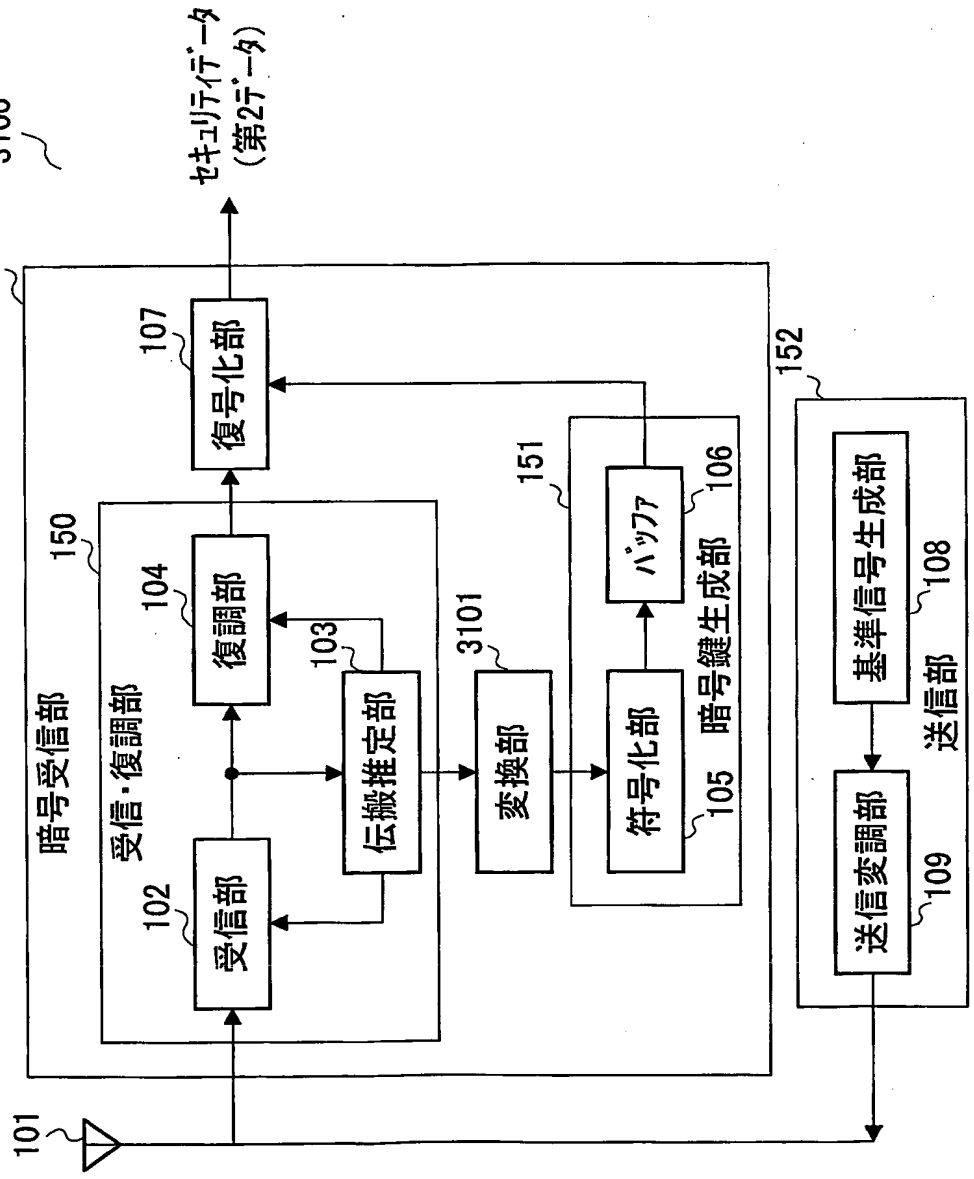

3100
セキュリティデータ
(第2データ)
153
107
復号化部
152
150
104
復調部
103
伝搬推定部
3101
変換部
151
パッファ
106
暗号鍵生成部
暗号受信部
受信・復調部
102
受信部
符号化部
105
基準信号生成部
108
送信部
送信変調部
109
101

図31

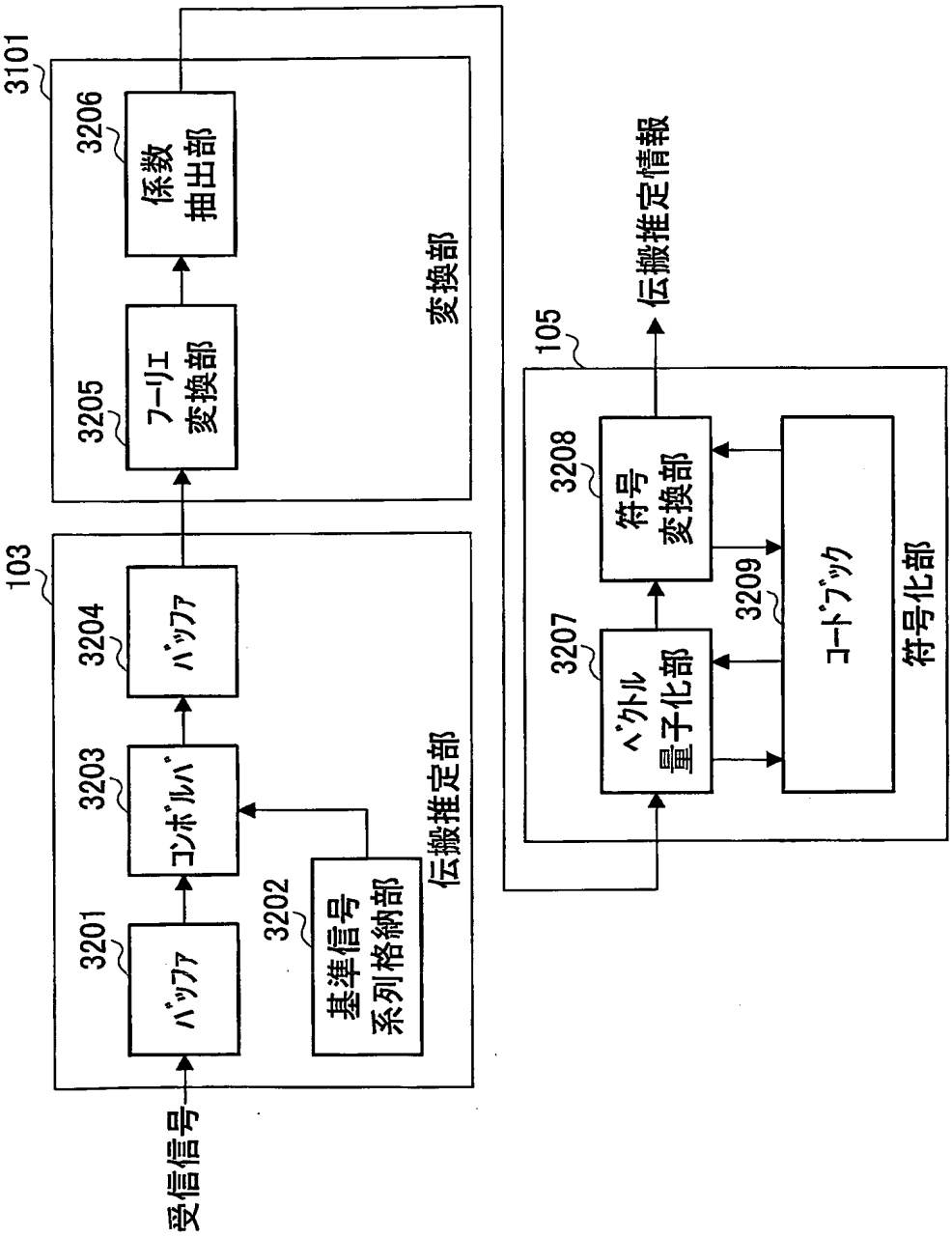

受信信号
103
伝搬推定部
3201
バッファ
3202
基準信号
系列格納部
3203
コンボルバ
3204
バッファ
3101
変換部
3205
フーリエ
変換部
3206
係数
抽出部
105
伝搬推定情報
符号化部
3207
ベクトル
量子化部
3208
符号
変換部
3209
コードブック

図32

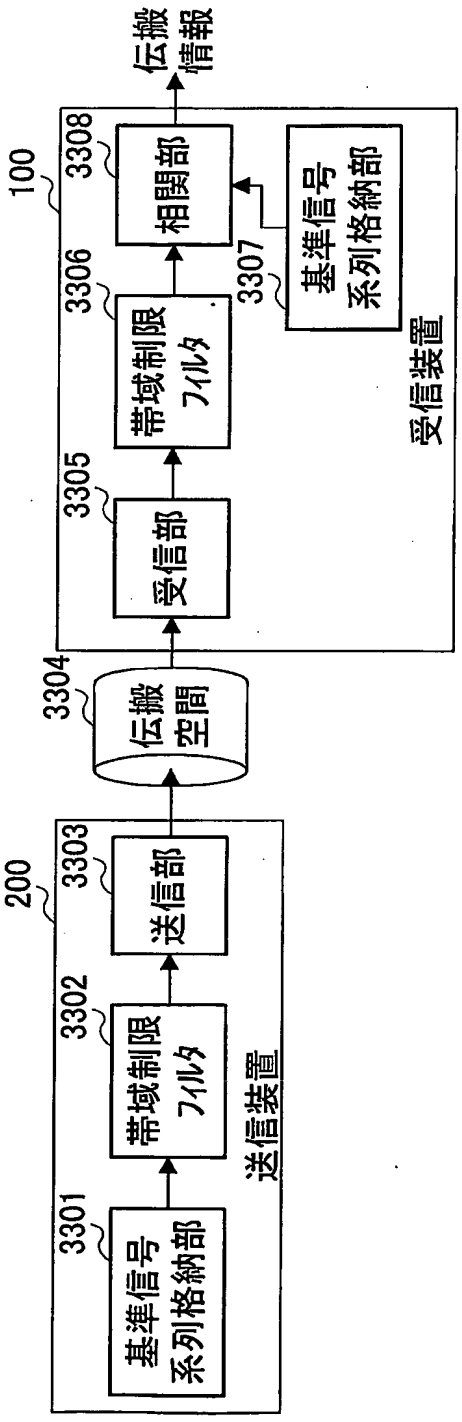

伝搬情報
100
3308
相関部
3307
基準信号系列格納部
3306
帯域制限フィルタ
受信装置
3305
受信部
3304
伝搬空間
200
3303
送信部
3302
帯域制限フィルタ
送信装置
3301
基準信号系列格納部

図33

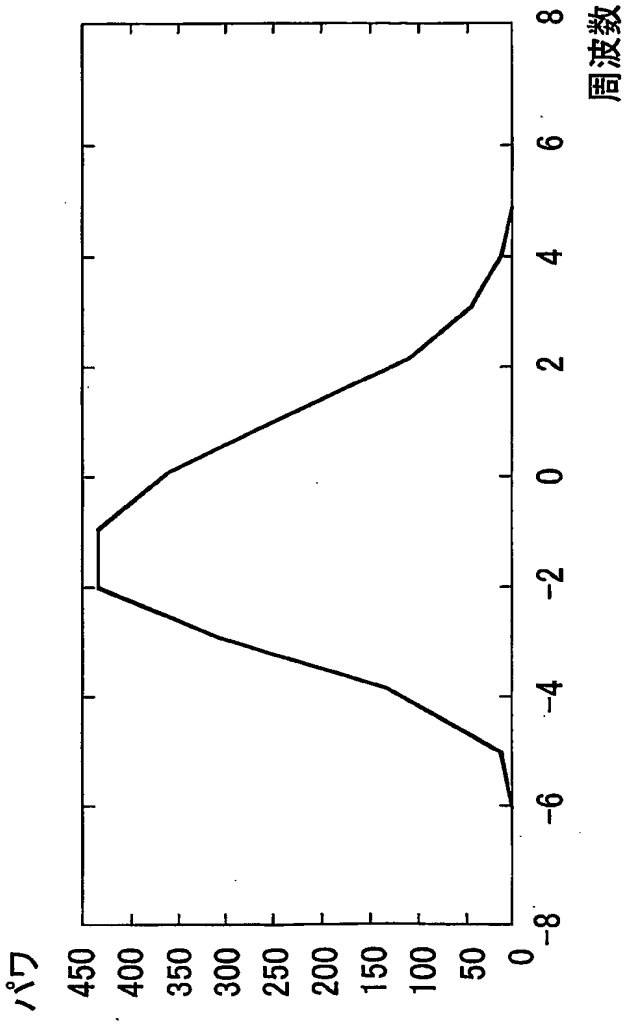


図34

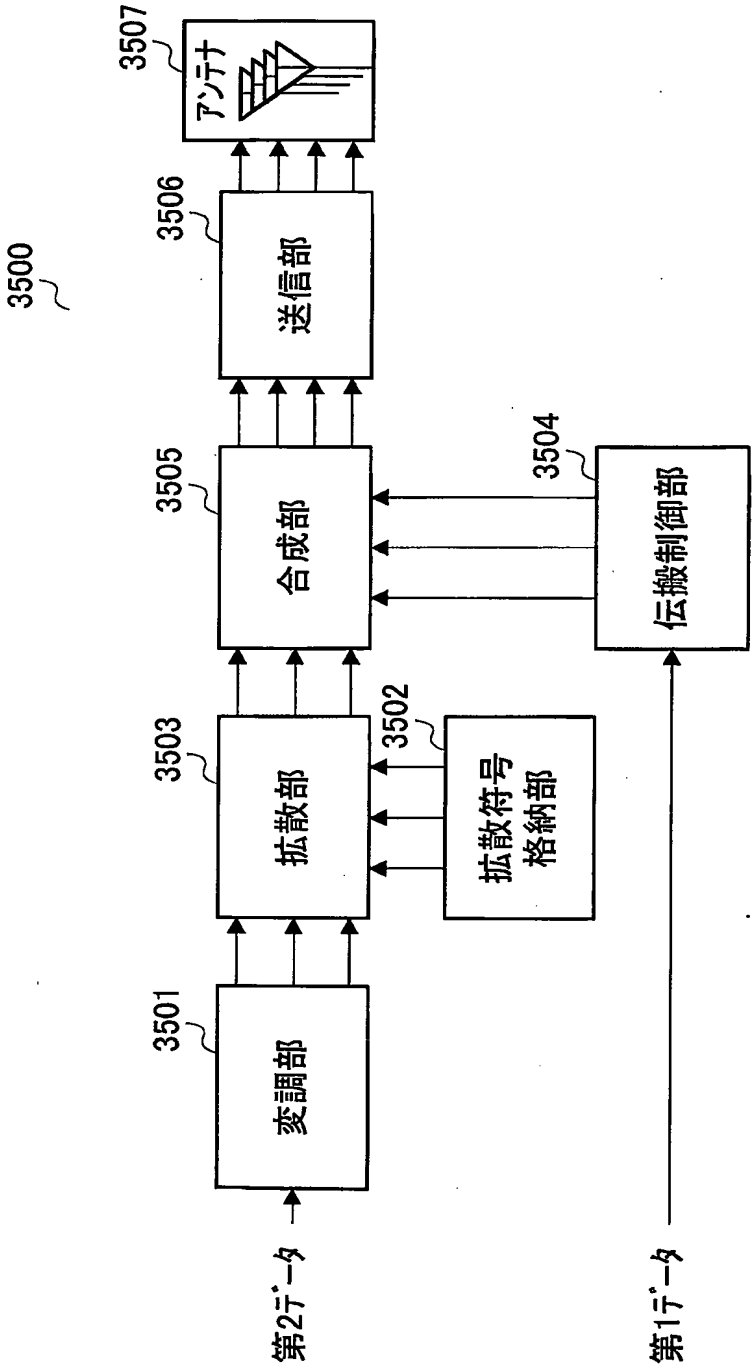

3500
3507
アンテナ
3506
送信部
3505
合成部
3504
伝搬制御部
3503
拡散部
3502
拡散符号格納部
3501
変調部
第2データ
第1データ

図35

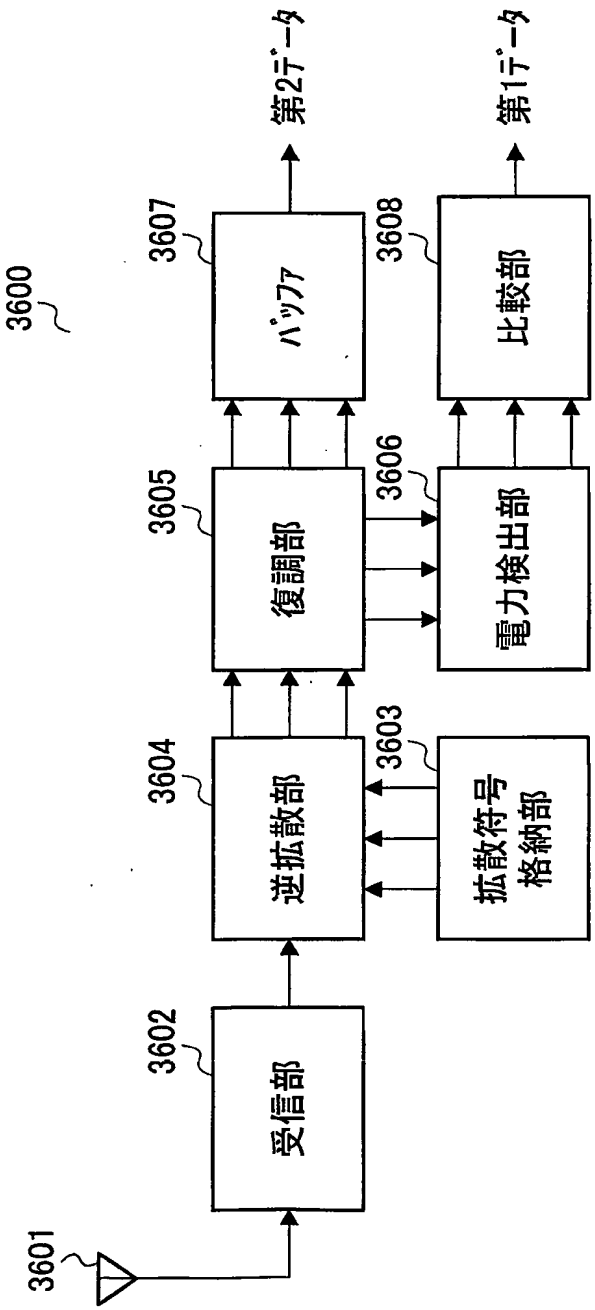

3600
3601
受信部
3602
逆拡散部
3604
拡散符号格納部
3603
復調部
3605
電力検出部
3606
バッファ
3607
比較部
3608
第2データ
第1データ

図36

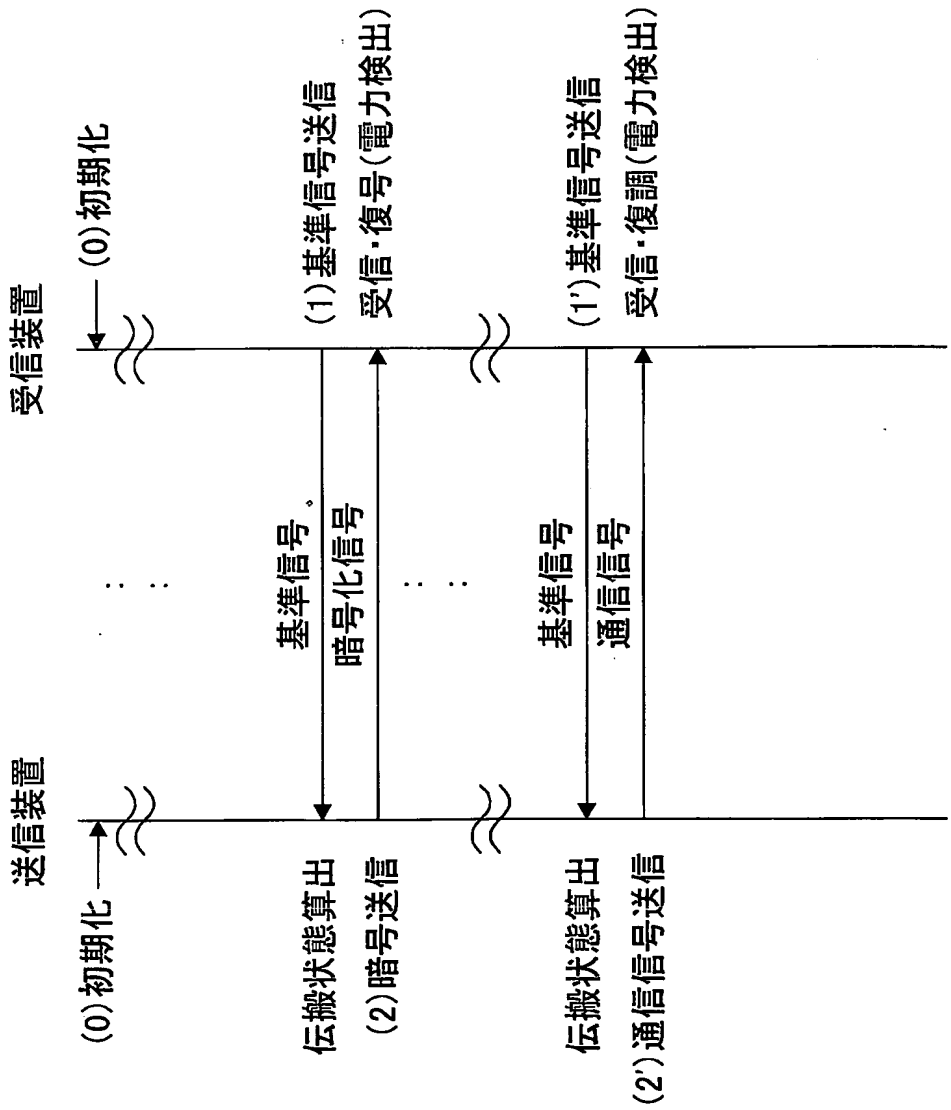

受信装置
(0)初期化
(1)基準信号送信
受信・復号(電力検出)
(1')基準信号送信
受信・復調(電力検出)
基準信号
暗号化信号
基準信号
通信信号
送信装置
(0)初期化
伝搬状態算出
(2)暗号送信
伝搬状態算出
(2')通信信号送信

図37

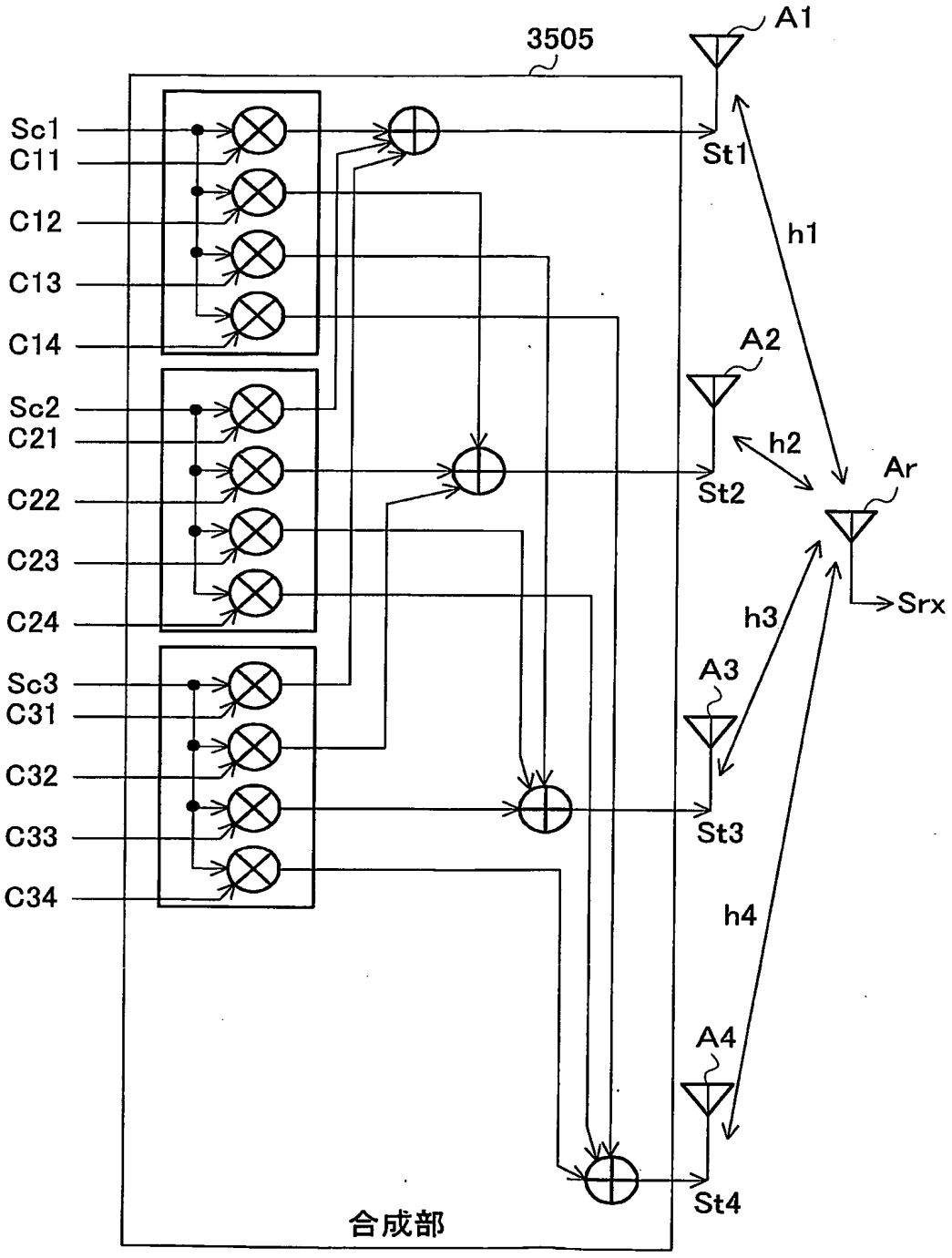

3505
A1
Sc1
C11
C12
C13
C14
St1
h1
A2
Sc2
C21
C22
C23
C24
h2
Ar
St2
Srx
h3
A3
Sc3
C31
C32
C33
C34
St3
h4
A4
St4
合成部

図38

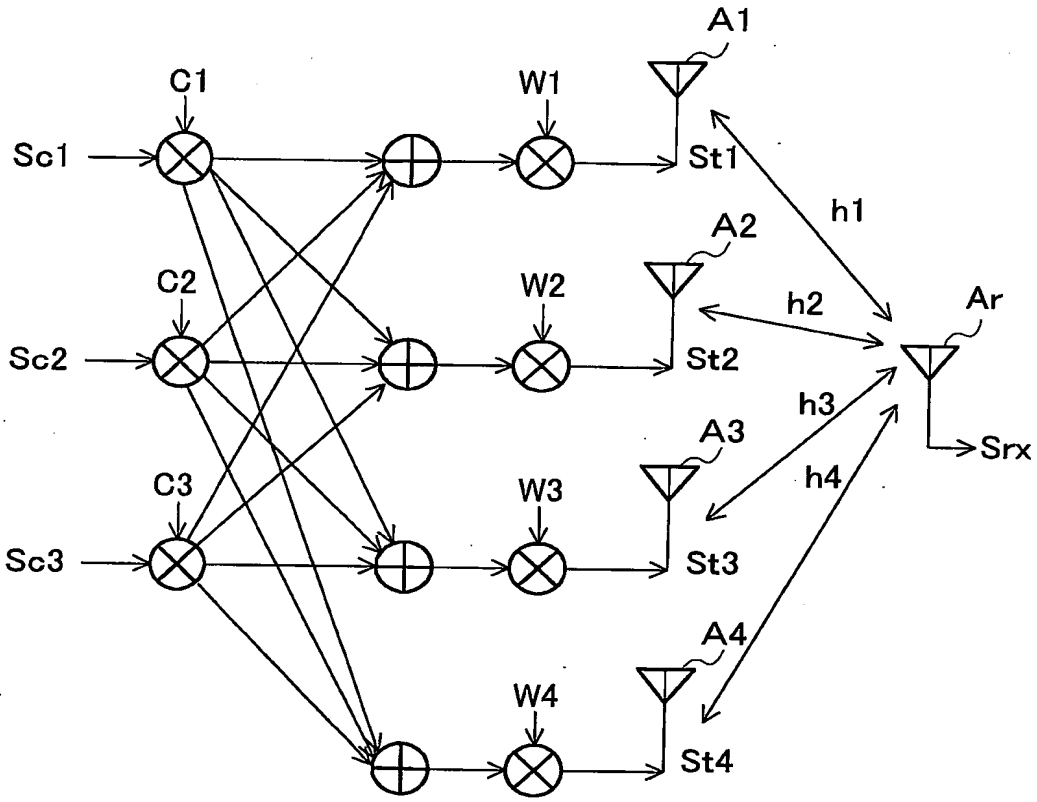

A1
C1
W1
Sc1
St1
h1
A2
C2
W2
h2
Ar
Sc2
St2
h3
A3
Srx
C3
W3
h4
Sc3
St3
A4
W4
St4

図39

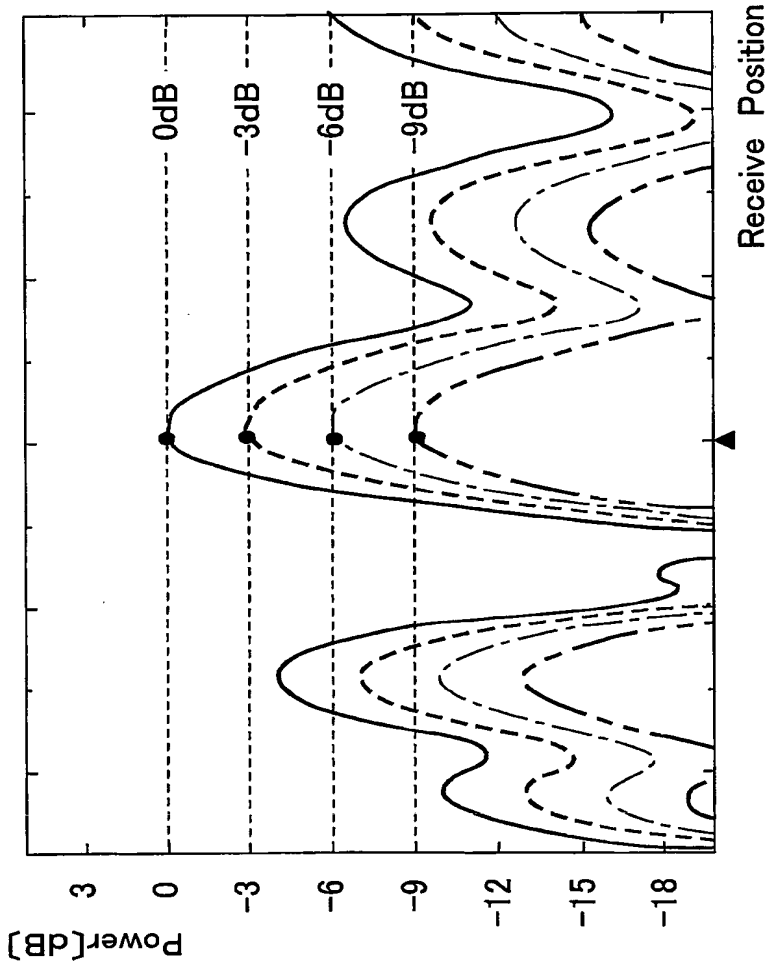


図40

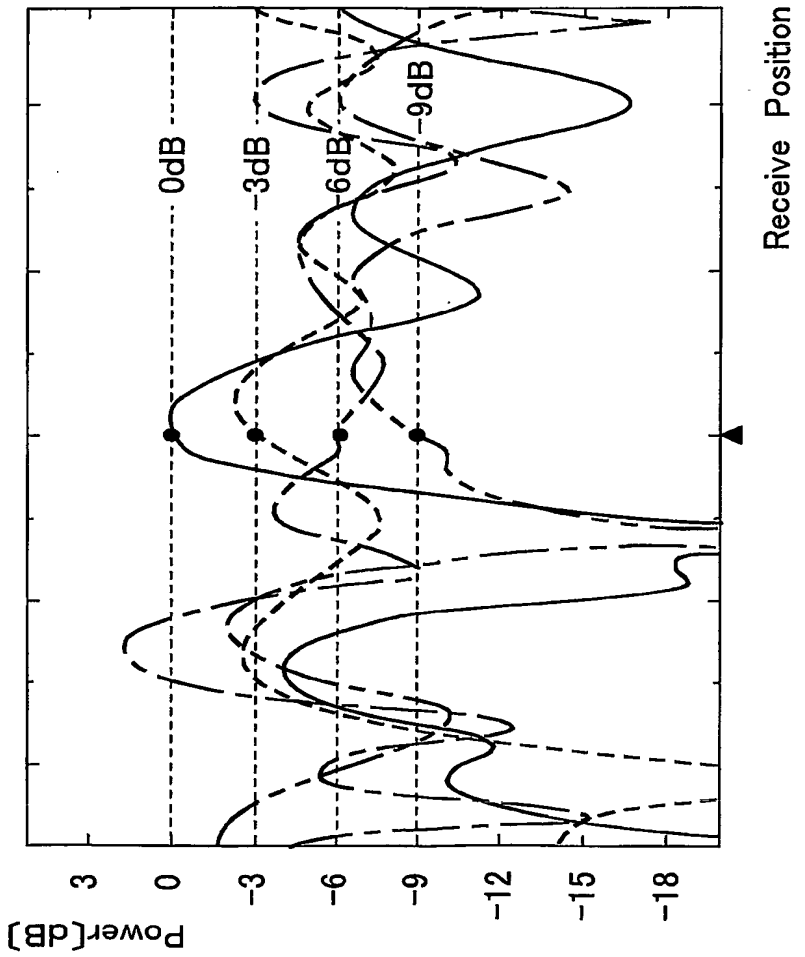


図41

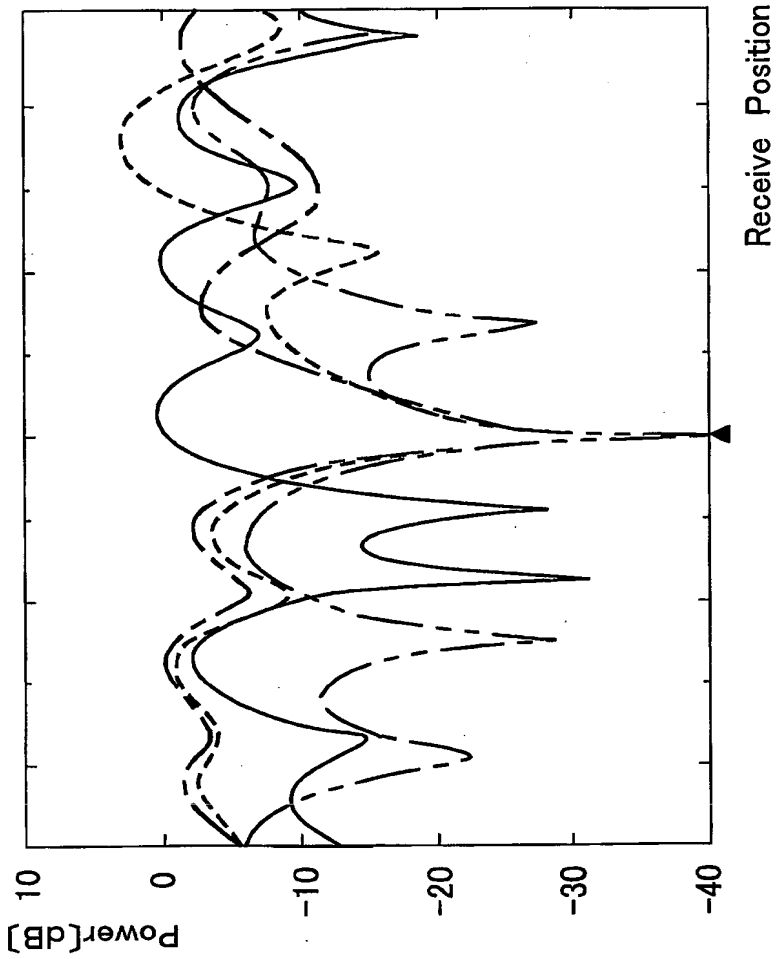


図42

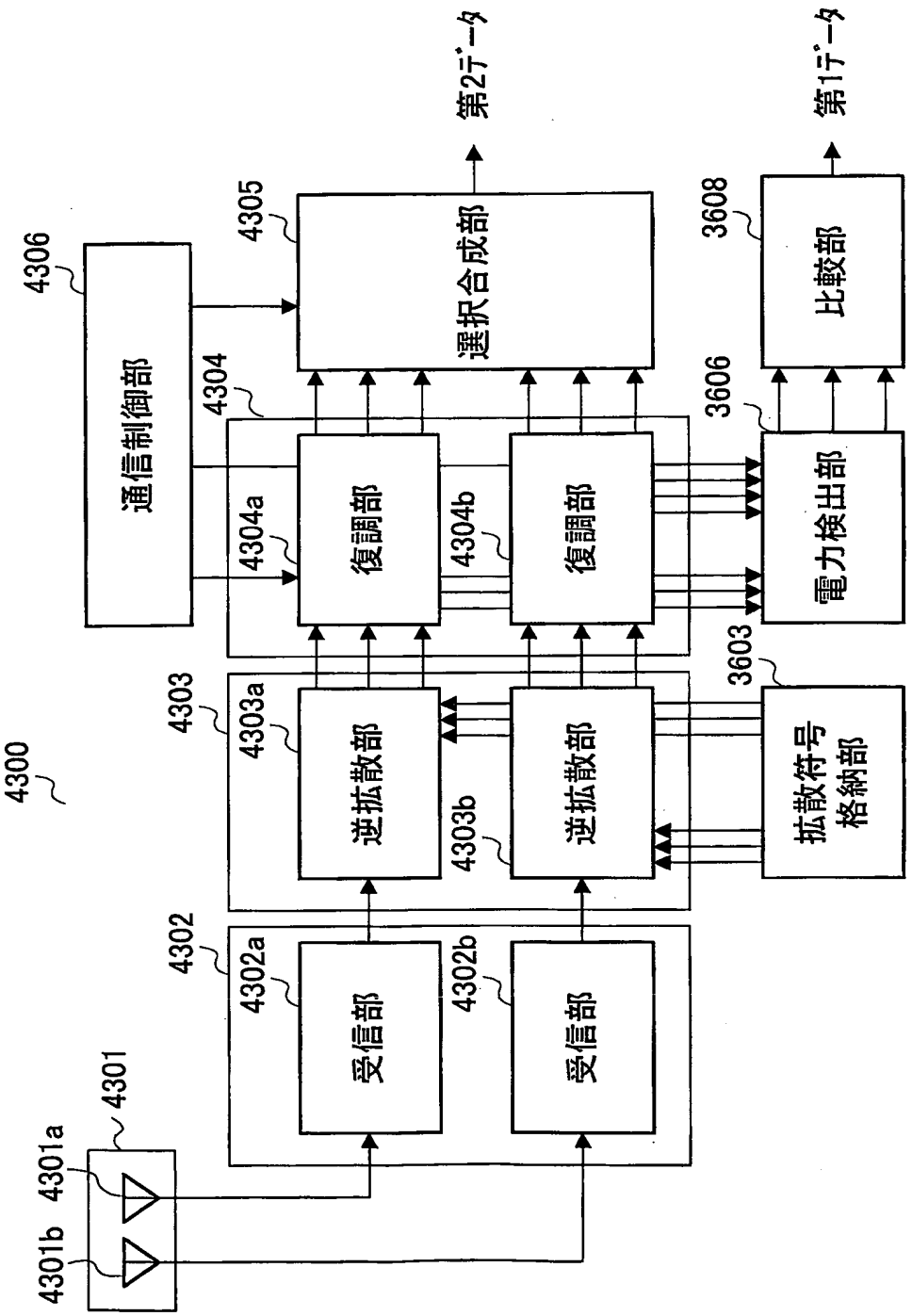

4300
4301
4301a
4301b
4302
4302a
4302b
受信部
受信部
4303
4303a
4303b
逆拡散部
逆拡散部
拡散符号
格納部
3603
4304
4304a
4304b
復調部
復調部
3606
電力検出部
3608
比較部
4305
選択合成部
第2データ
第1データ
4306
通信制御部

図43

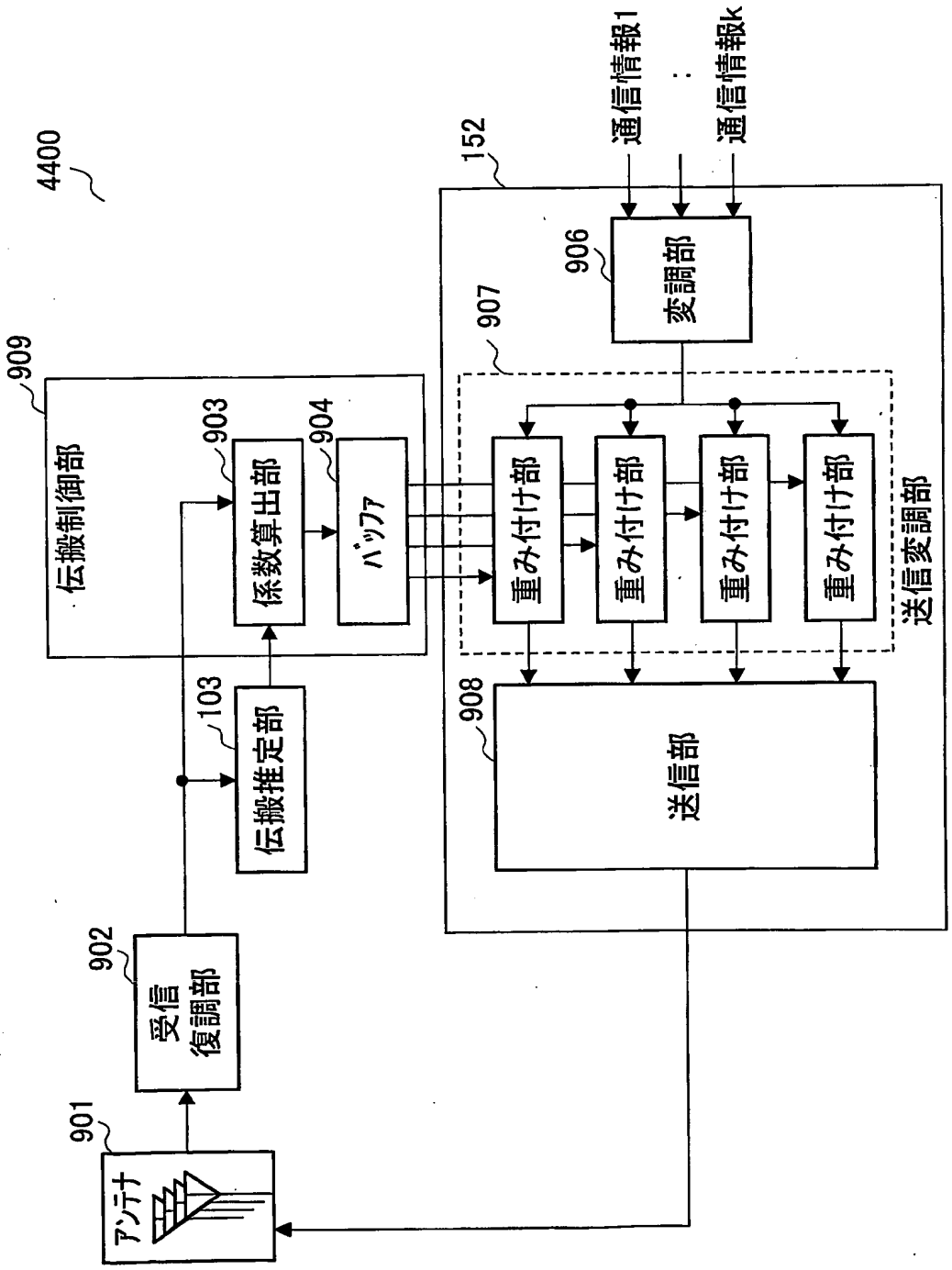

4400
152
通信情報1
通信情報k
906
変調部
907
909
伝搬制御部
903
係数算出部
904
バッファ
重み付け部
重み付け部
重み付け部
重み付け部
送信変調部
103
伝搬推定部
908
送信部
902
受信
復調部
901
アンテナ

図44

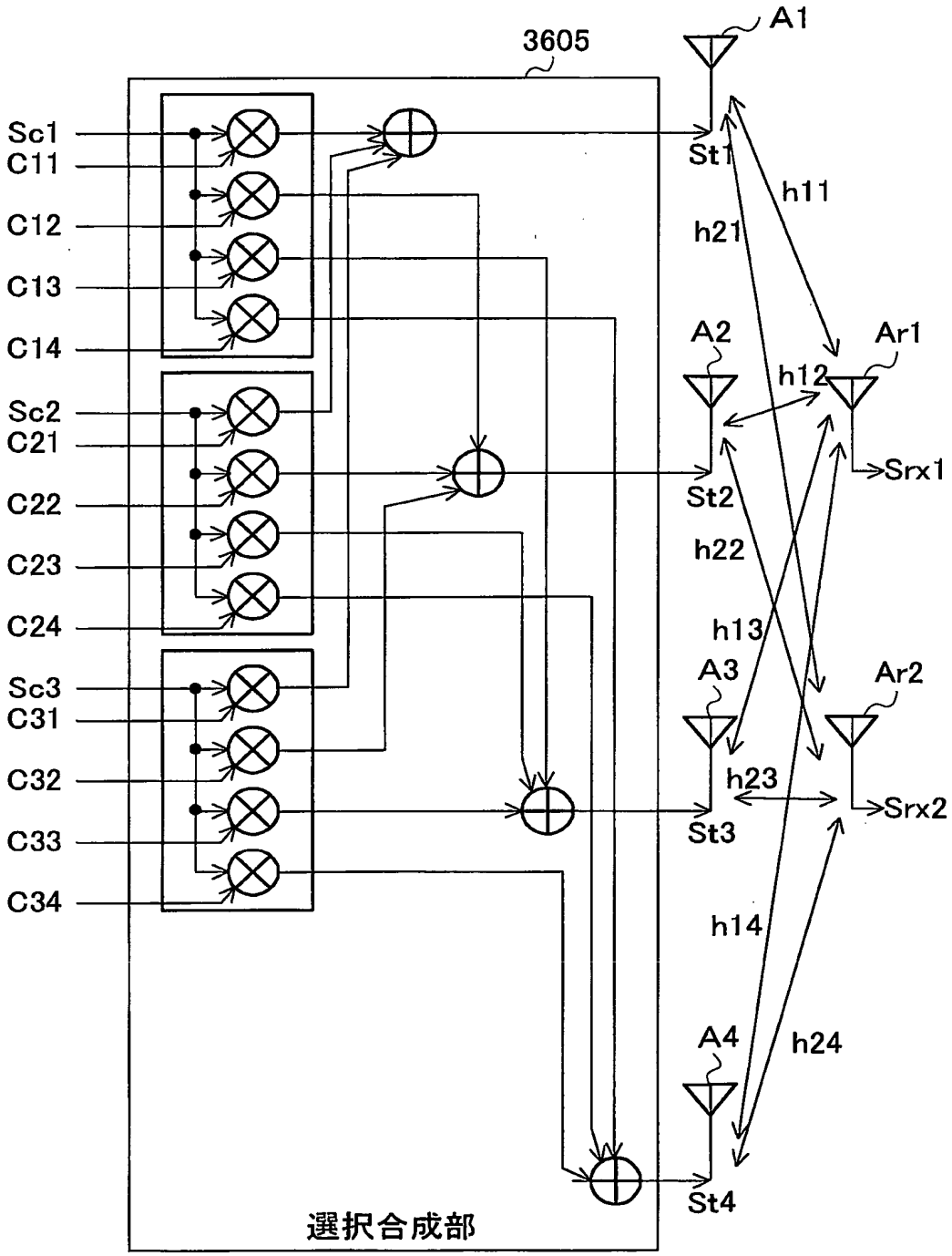

3605
A1
Sc1
C11
C12
C13
C14
Sc2
C21
C22
C23
C24
Sc3
C31
C32
C33
C34
St1
h11
h21
A2
Ar1
h12
Srx1
St2
h22
h13
A3
Ar2
h23
Srx2
St3
h14
A4
h24
St4
選択合成部

図45

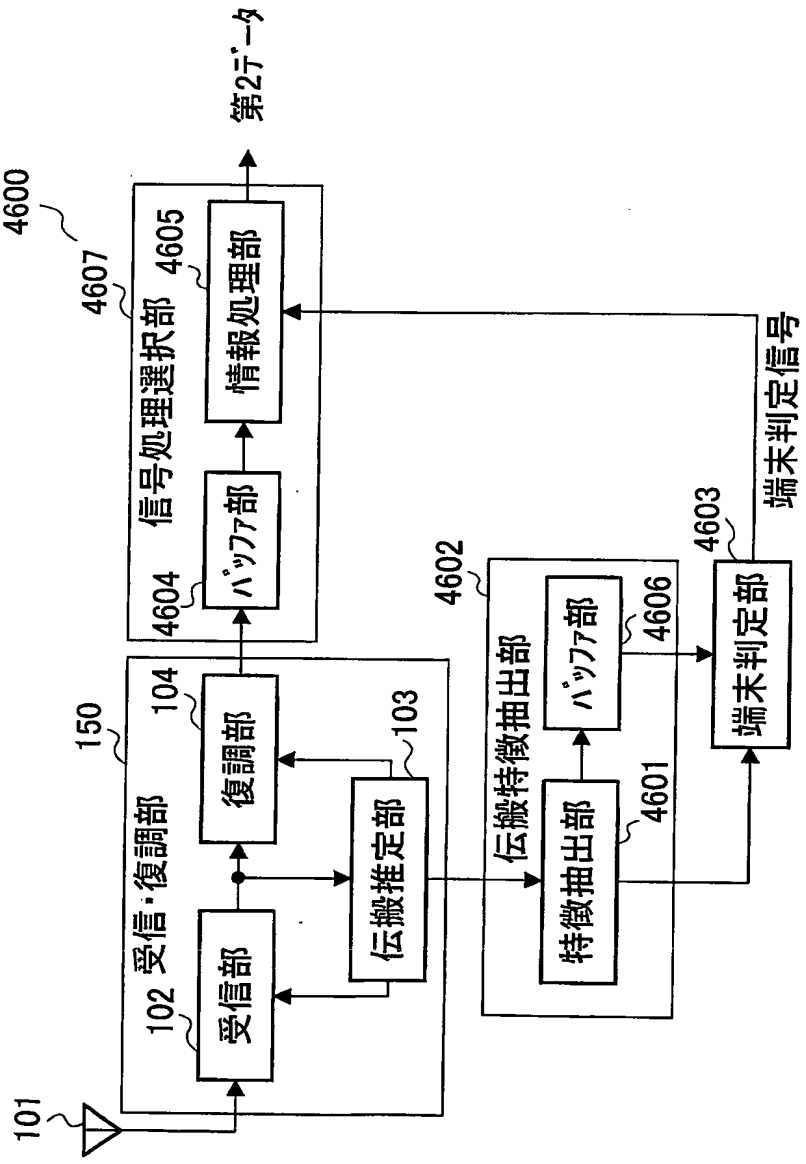

4600
4607
信号処理選択部
4605
情報処理部
第2データ
4604
バッファ部
150
受信・復調部
104
復調部
103
伝搬推定部
102
受信部
101
4602
伝搬特徴抽出部
バッファ部
4606
特徴抽出部
4601
4603
端末判定部
端末判定信号

図46

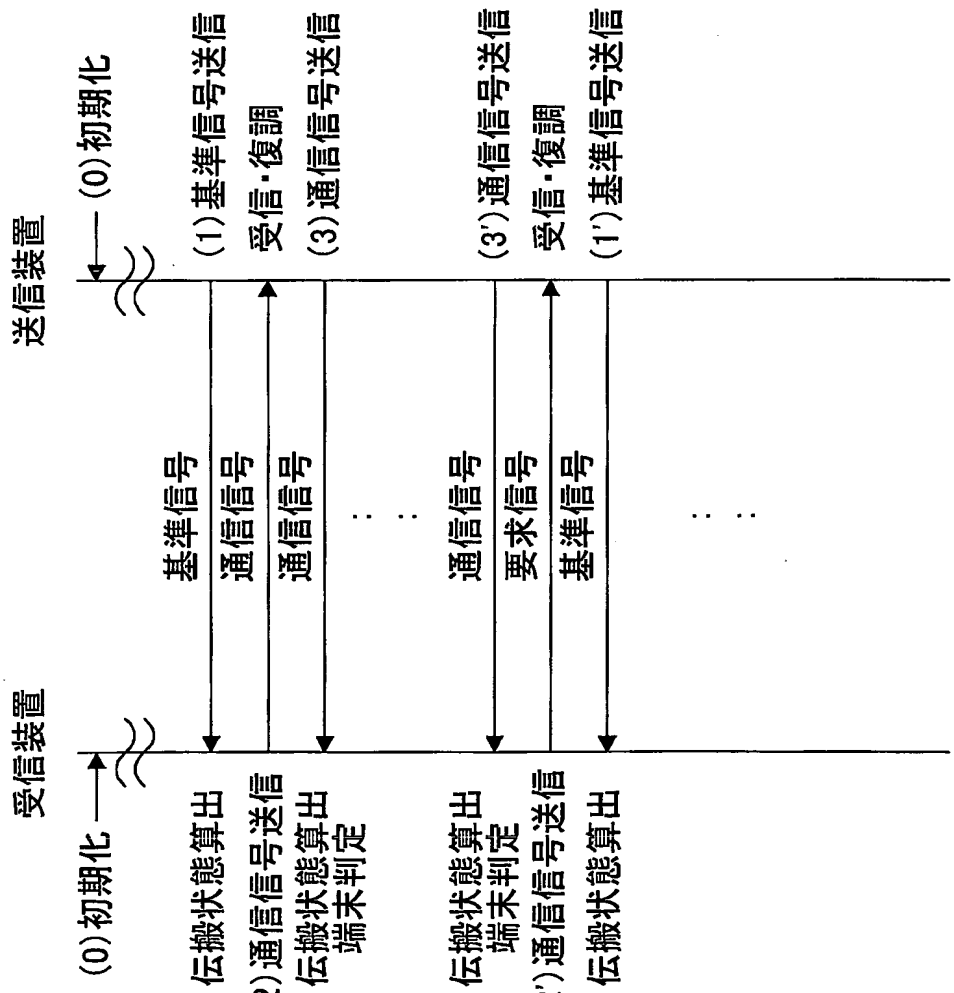

送信装置
受信装置
(0)初期化
(0)初期化
(1)基準信号送信
受信・復調
(3)通信信号送信
(3')通信信号送信
受信・復調
(1')基準信号送信
基準信号
通信信号
通信信号
通信信号
要求信号
基準信号
伝搬状態算出
(2)通信信号送信
伝搬状態算出
端末判定
伝搬状態算出
端末判定
(2')通信信号送信
伝搬状態算出

図47

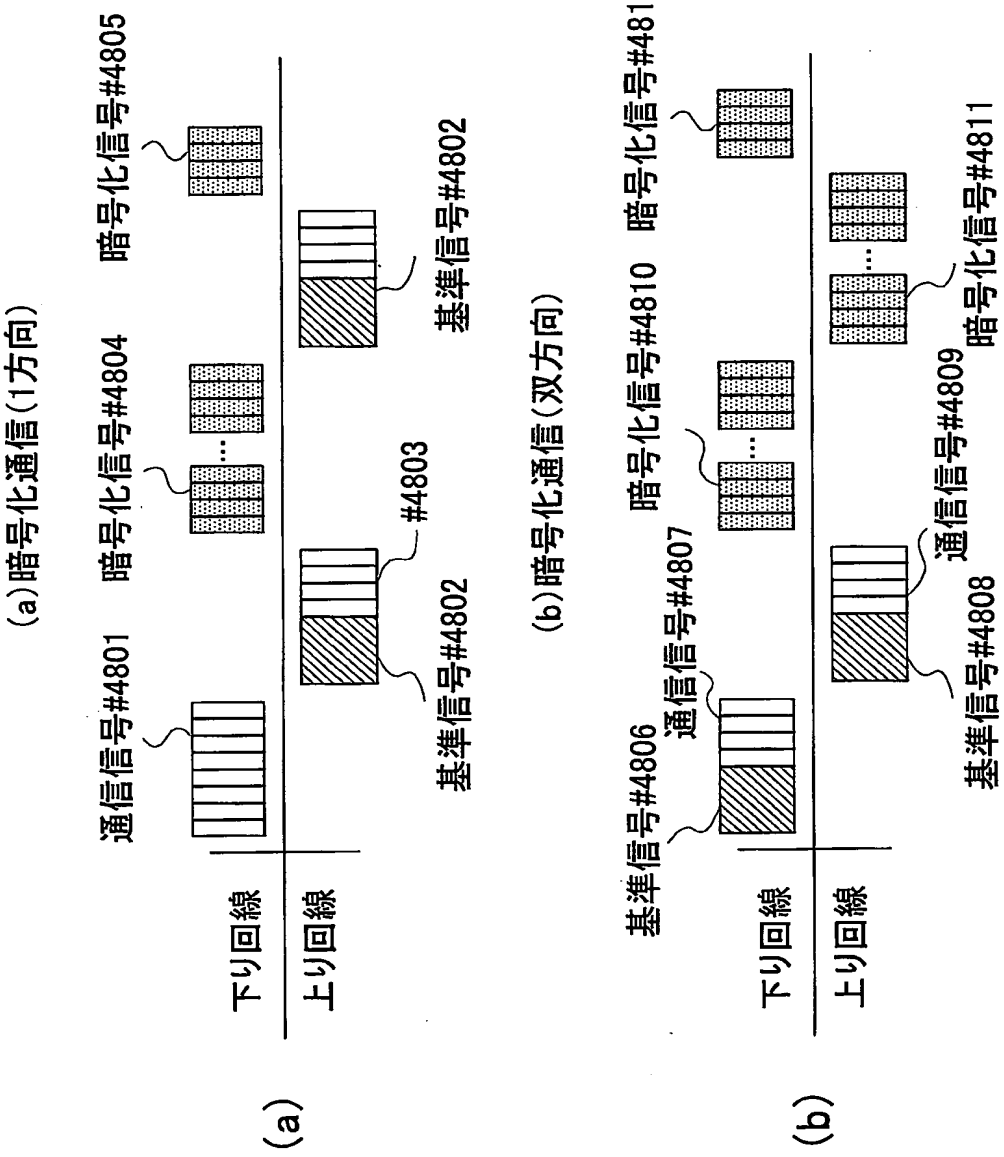

(a)暗号化通信(1方向)
通信信号#4801
暗号化信号#4804
暗号化信号#4805
#4803
基準信号#4802
基準信号#4802
下り回線
上り回線
(a)
(b)暗号化通信(双方向)
基準信号#4806
通信信号#4807
暗号化信号#4810
暗号化信号#4812
通信信号#4809
基準信号#4808
暗号化信号#4811
下り回線
上り回線
(b)

図48

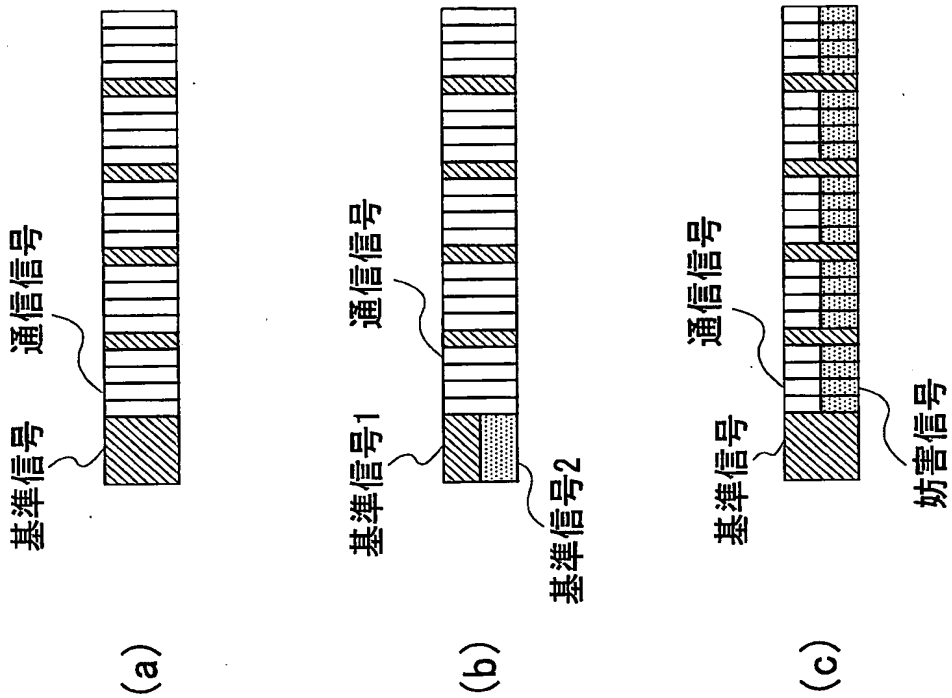


図49

(a)フレーム構成1

パイロット信号	データn	データn	データn	データn	データn
	:	:	:	:	:
	データ2	データ2	データ2	データ2	データ2
	データ1	データ1	データ1	データ1	データ1

(b)フレーム構成2

データn	データn	データn	データn	データn	データn
:	:	:	:	:	:
データ1	データ1	データ1	データ1	データ1	データ1
パイロット信号	パイロット信号	パイロット信号	パイロット信号	パイロット信号	パイロット信号

(c)フレーム構成3

データn	データn	データn	データn	データn	データn
:	:	:	:	:	:
パイロット信号m	パイロット信号m	パイロット信号m	パイロット信号m	パイロット信号m	パイロット信号m
:	:	:	:	:	:
データ1	データ1	データ1	データ1	データ1	データ1
パイロット信号1	パイロット信号1	パイロット信号1	パイロット信号1	パイロット信号1	パイロット信号1

図50

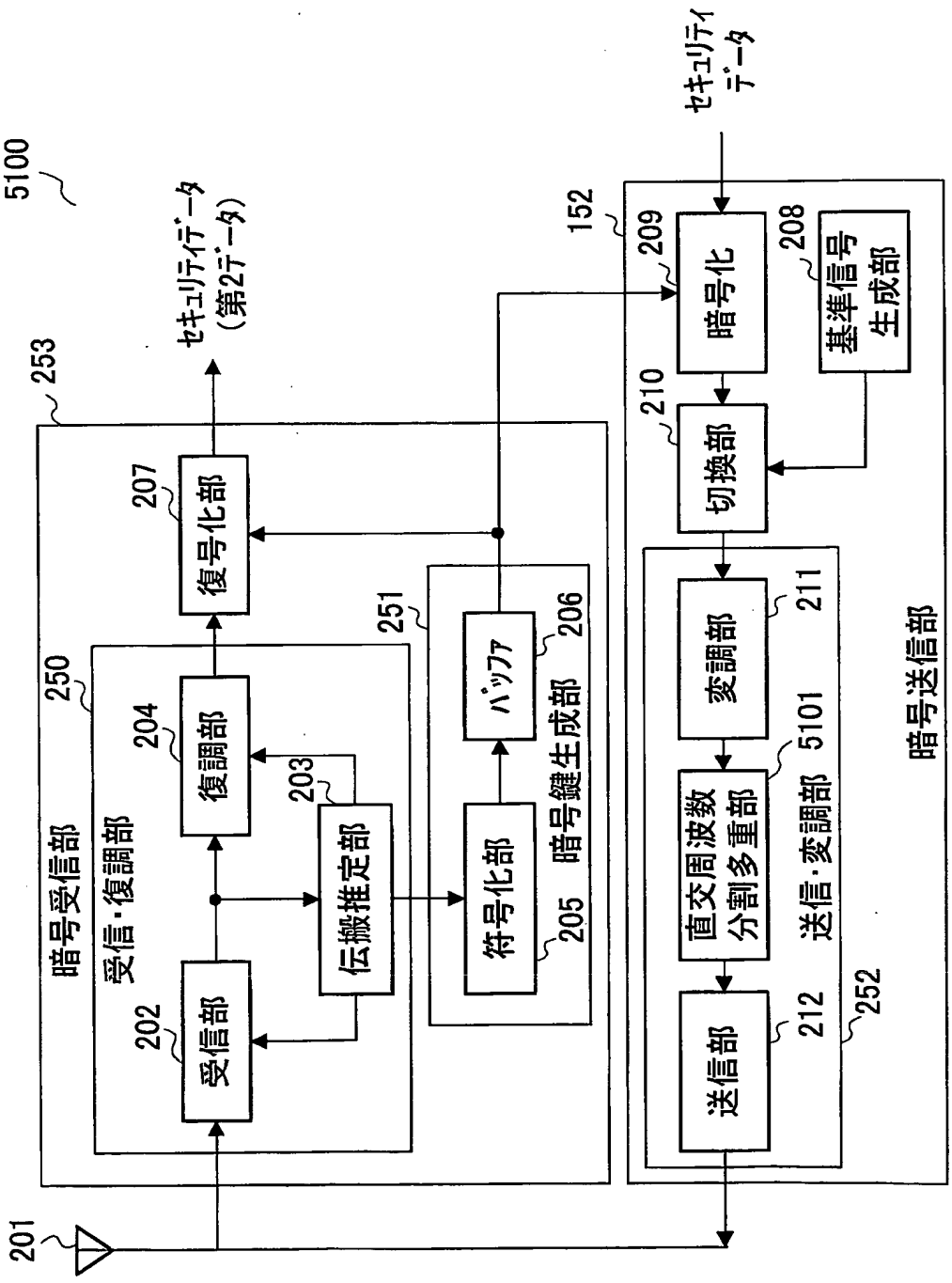

5100
セキュリティデータ
(第2データ)
セキュリティ
データ
253
152
207
復号化部
209
暗号化
208
基準信号
生成部
210
切換部
250
暗号受信部
受信・復調部
204
復調部
203
伝搬推定部
251
バッファ
206
暗号鍵生成部
変調部
211
直交周波数
分割多重部
5101
送信・変調部
暗号送信部
202
受信部
205
符号化部
送信部
212
252
201

図51

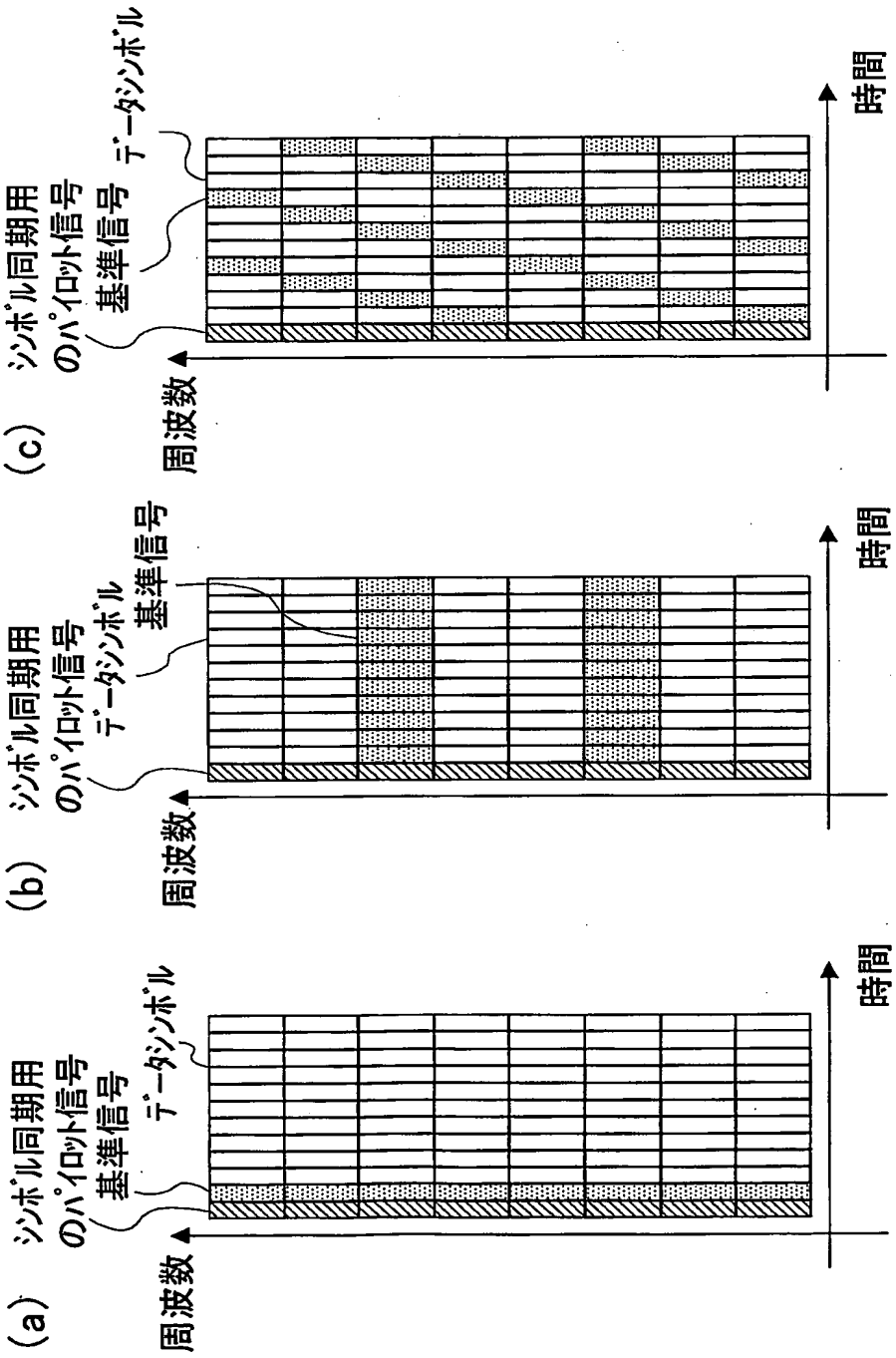

(a)
シンボル同期用
のパイロット信号
基準信号
データシンボル
周波数
時間
(b)
シンボル同期用
のパイロット信号
データシンボル
基準信号
周波数
時間
(c)
シンボル同期用
のパイロット信号
基準信号
データシンボル
周波数
時間

図52

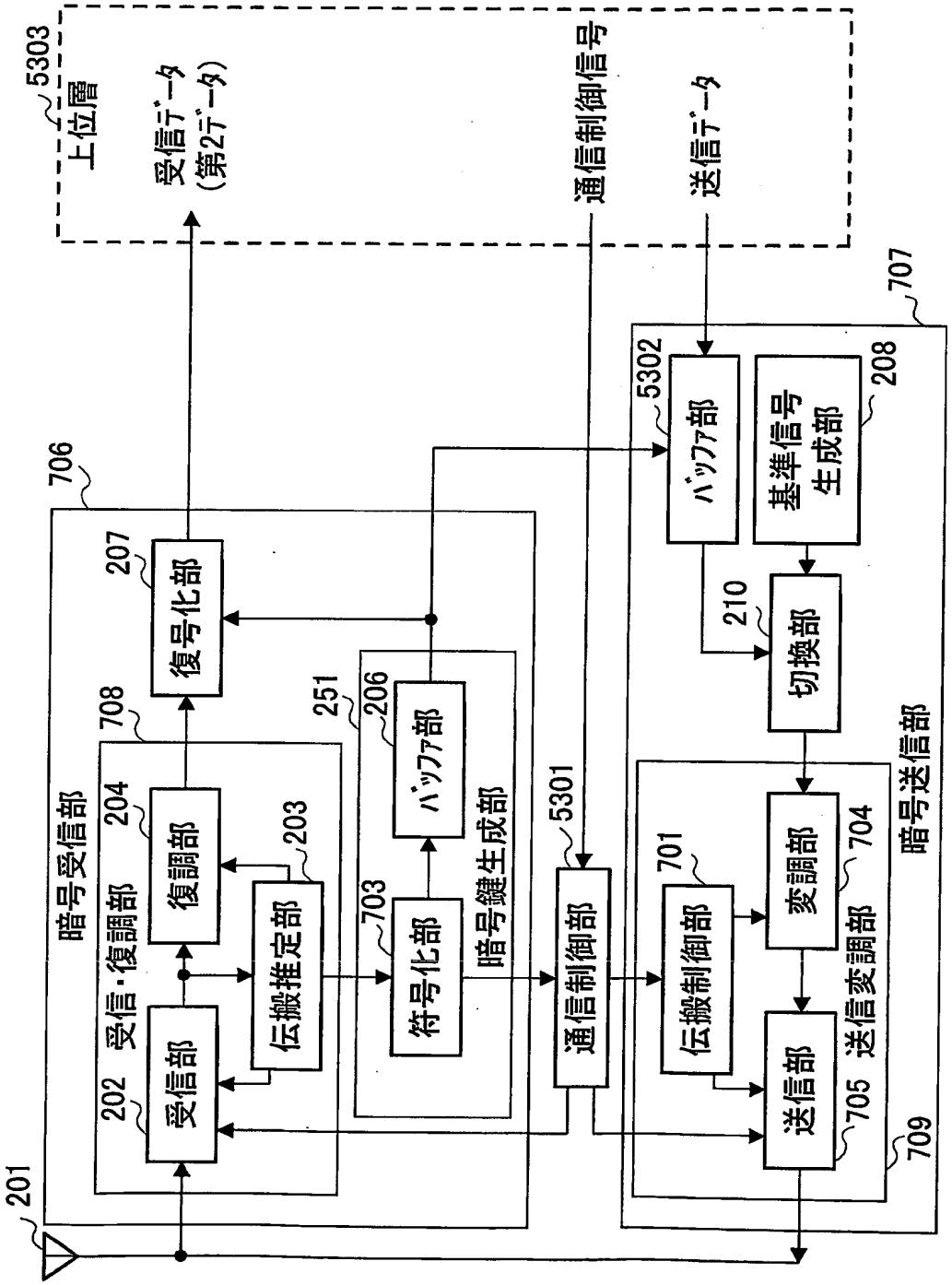

5303
上位層
受信データ
(第2データ)
通信制御信号
送信データ
707
5302
バッファ部
208
基準信号
生成部
706
207
復号化部
210
切換部
708
251
206
バッファ部
暗号受信部
204
復調部
203
伝搬推定部
703
符号化部
暗号鍵生成部
5301
通信制御部
701
伝搬制御部
変調部
704
暗号送信部
202
受信部
送信部
705
送信変調部
709
201

図53

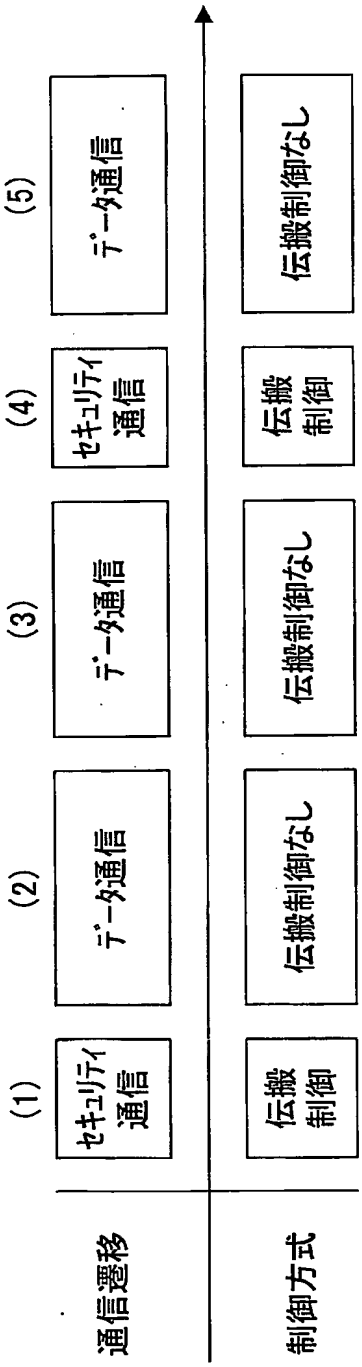

(1)
(2)
(3)
(4)
(5)
セキュリティ通信
データ通信
データ通信
セキュリティ通信
データ通信
伝搬制御
伝搬制御なし
伝搬制御なし
伝搬制御
伝搬制御なし
通信遷移
制御方式

図54

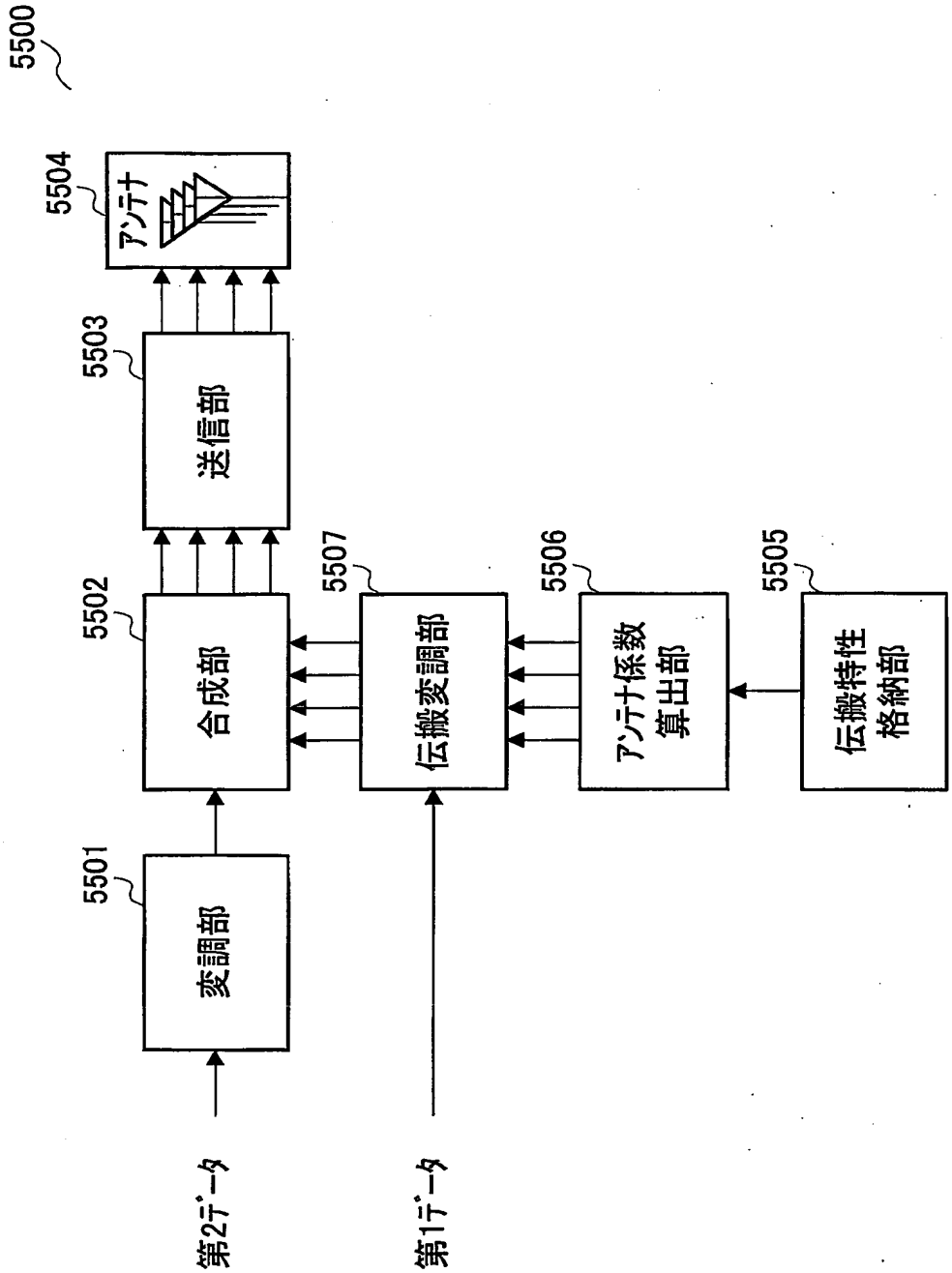

5500
5504
アンテナ
5503
送信部
5502
合成部
5507
伝搬変調部
5506
アンテナ係数
算出部
5505
伝搬特性
格納部
5501
変調部
第2データ
第1データ

図55

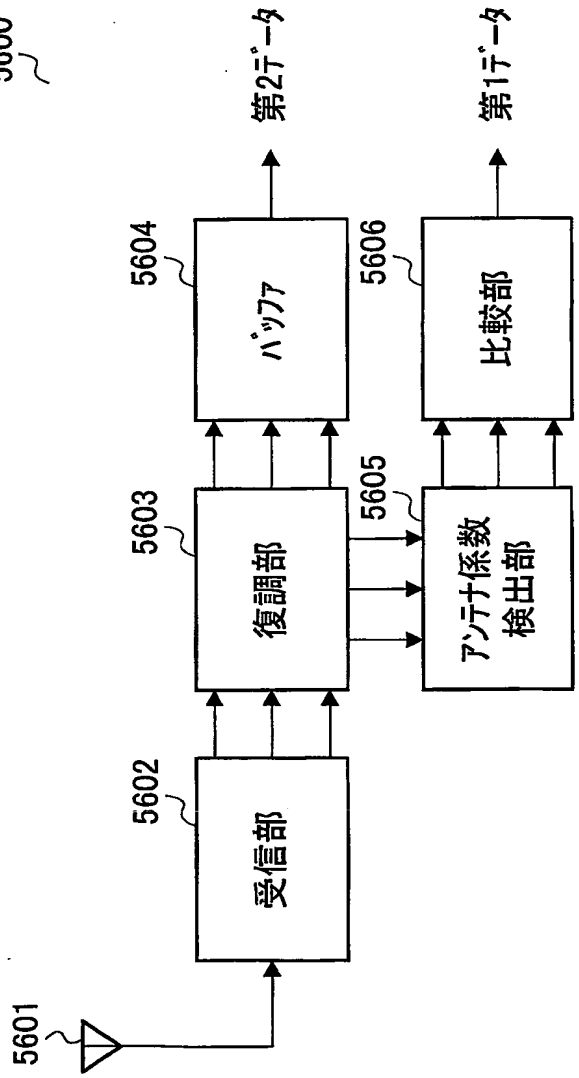

5600
第2データ
第1データ
5604
バッファ
5606
比較部
5603
復調部
5605
アンテナ係数
検出部
5602
受信部
5601

図56

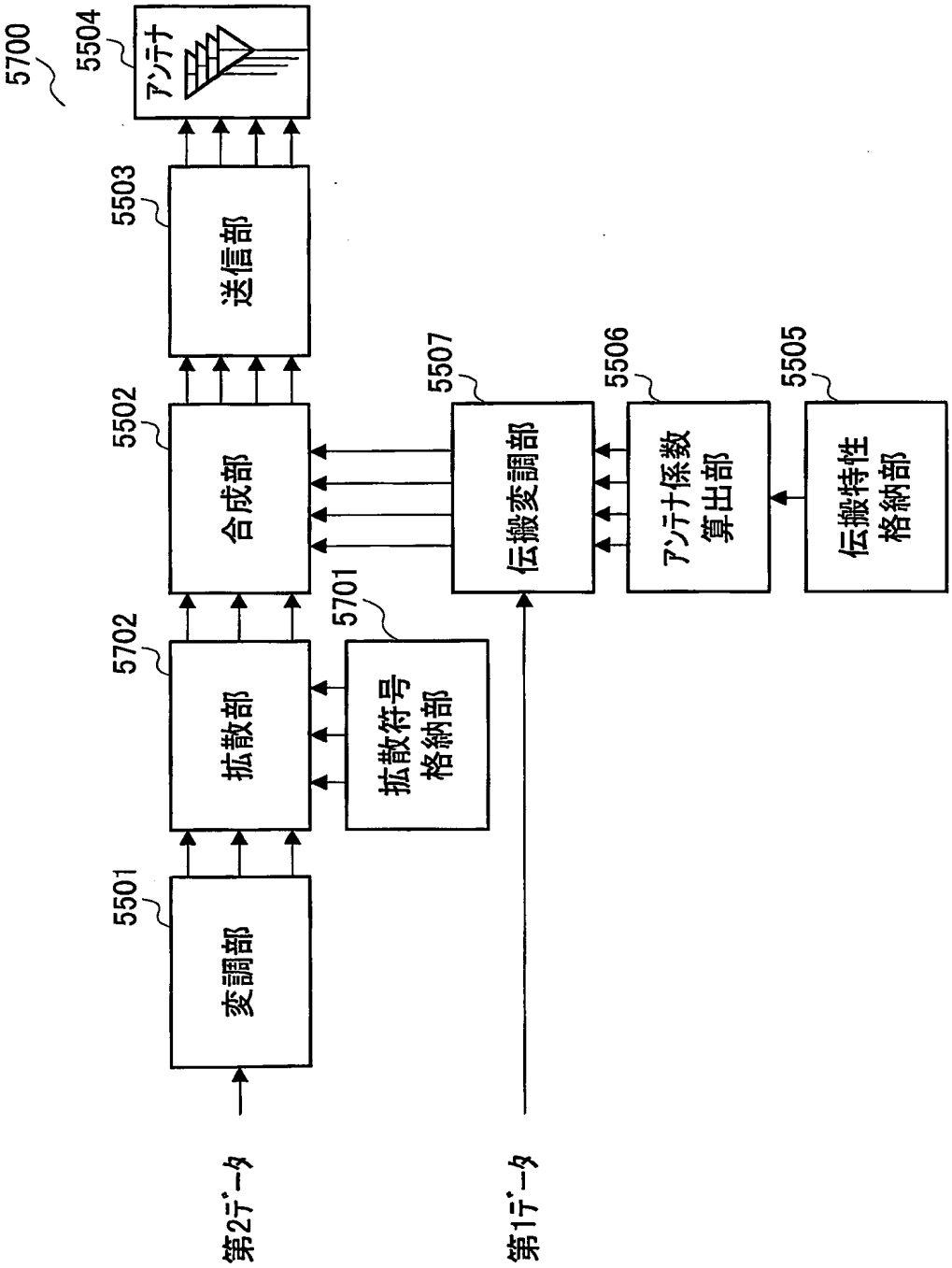

5700
5504
アンテナ
5503
送信部
5502
合成部
5507
伝搬変調部
5506
アンテナ係数
算出部
5505
伝搬特性
格納部
5701
拡散符号
格納部
5702
拡散部
5501
変調部
第2データ
第1データ

図57

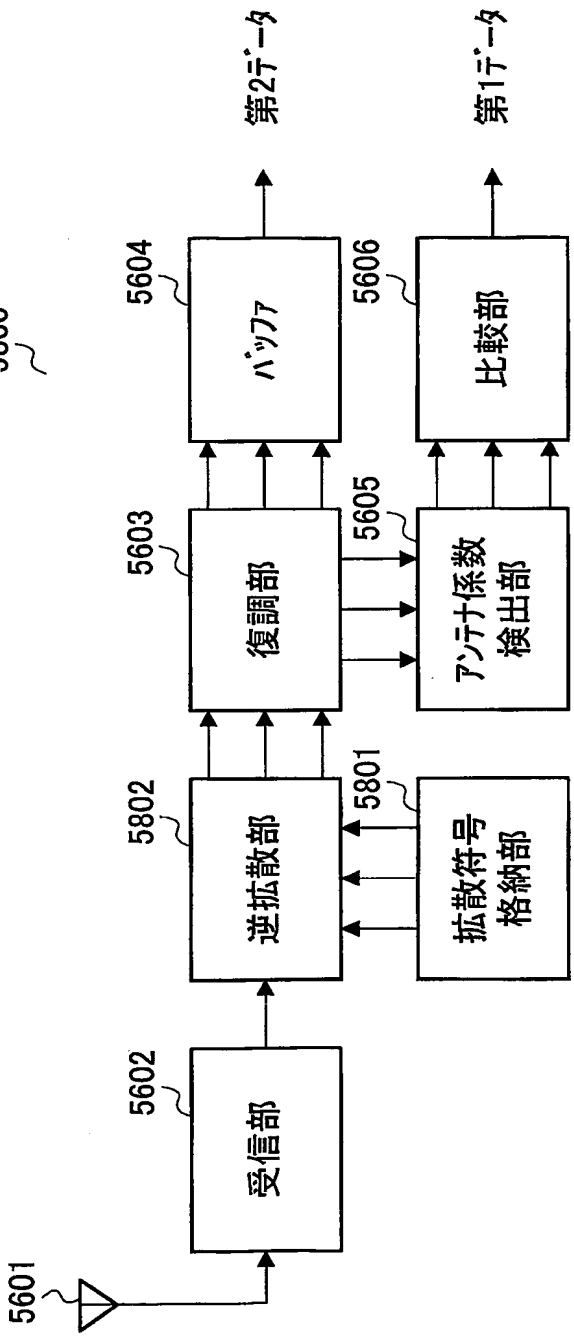

5800
5601
5602
受信部
5802
逆拡散部
5801
拡散符号
格納部
5603
復調部
5605
アンテナ係数
検出部
5604
バッファ
5606
比較部
第2データ
第1データ

図58

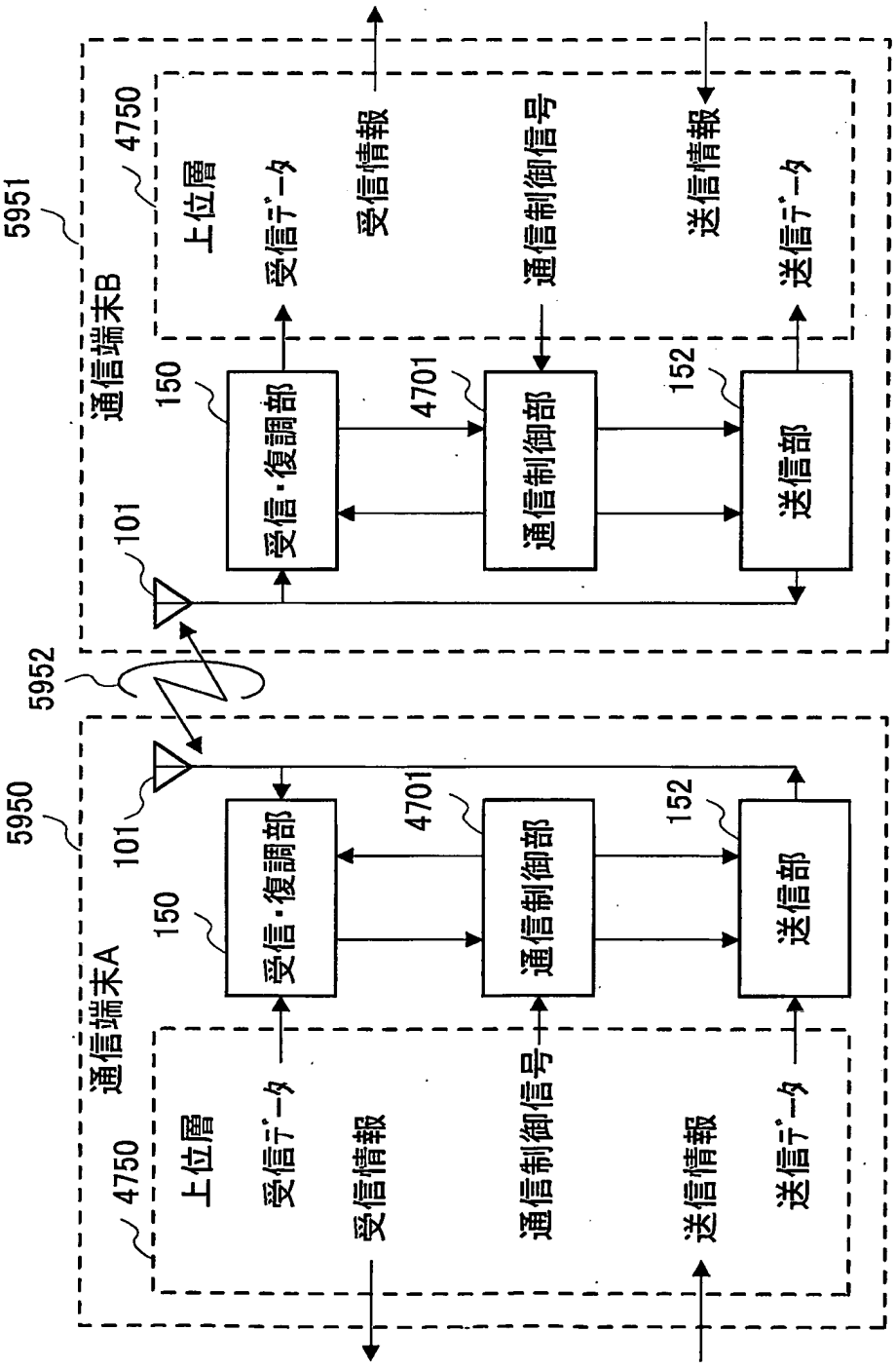

5951
通信端末B
4750
上位層
受信ﾃﾞｰﾀ
受信情報
通信制御信号
送信情報
送信ﾃﾞｰﾀ
150
受信・復調部
4701
通信制御部
152
送信部
101
5952
5950
通信端末A
4750
上位層
受信ﾃﾞｰﾀ
受信情報
通信制御信号
送信情報
送信ﾃﾞｰﾀ
150
受信・復調部
4701
通信制御部
152
送信部
101

図59

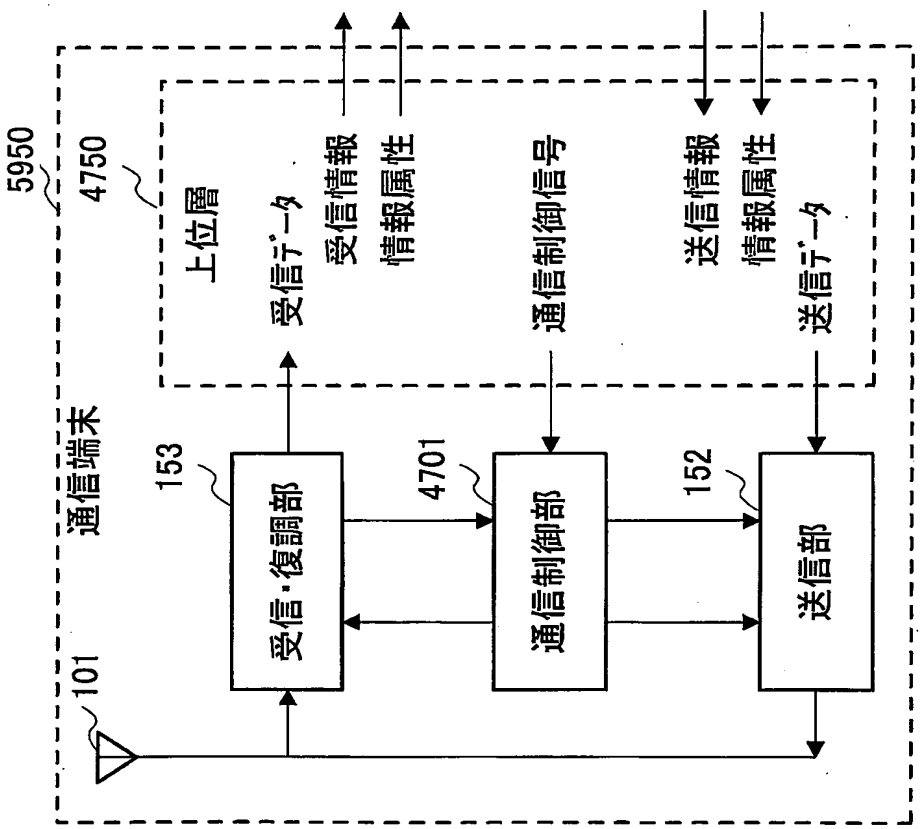

5950
通信端末
4750
上位層
受信データ
受信情報
情報属性
通信制御信号
送信情報
情報属性
送信データ
153
受信・復調部
4701
通信制御部
152
送信部
101

図60

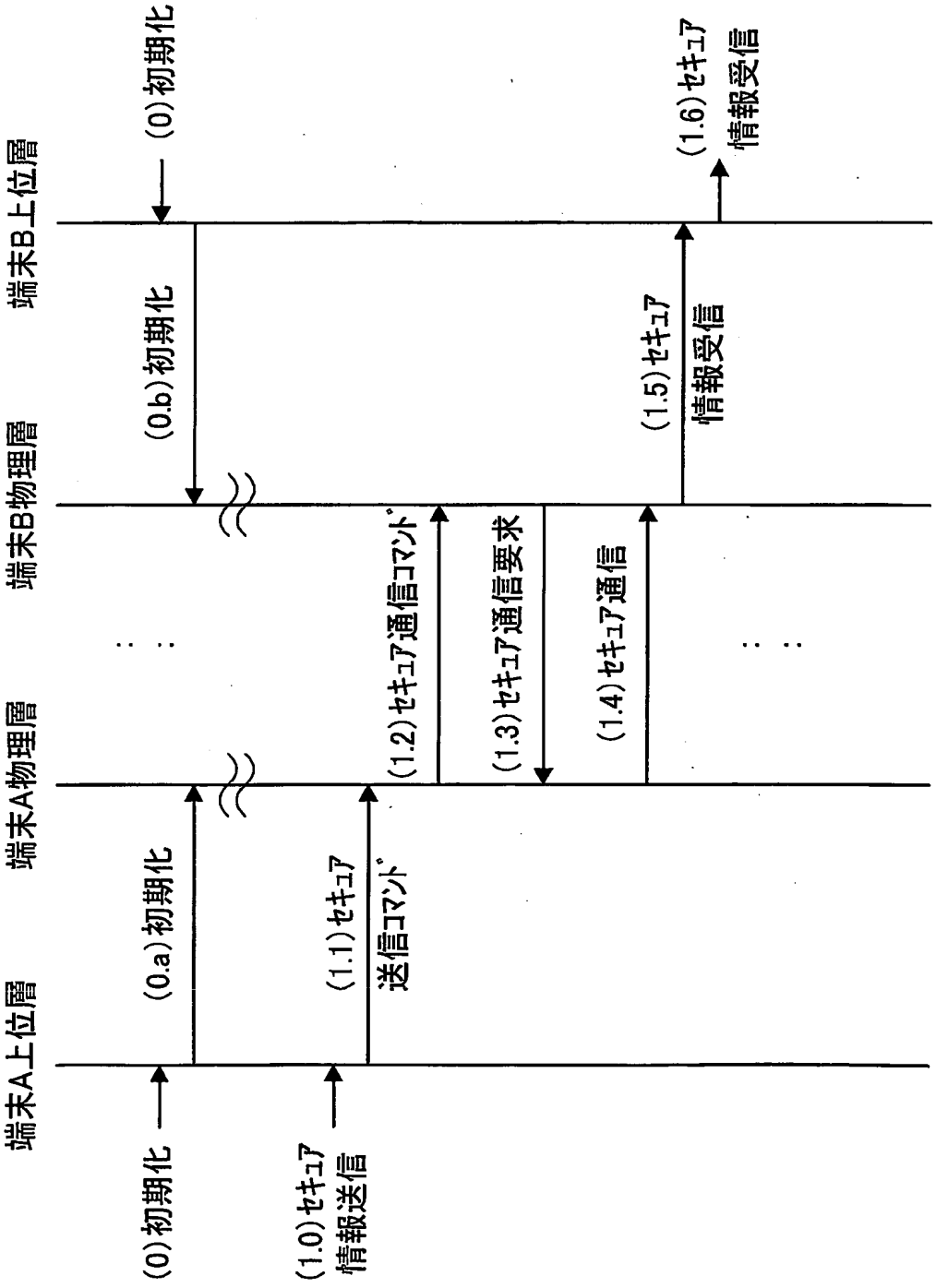

端末A上位層
端末A物理層
端末B物理層
端末B上位層
(0)初期化
(0.a)初期化
(0.b)初期化
(0)初期化
(1.0)セキュア情報送信
(1.1)セキュア送信コマンド
(1.2)セキュア通信コマンド
(1.3)セキュア通信要求
(1.4)セキュア通信
(1.5)セキュア情報受信
(1.6)セキュア情報受信

図61

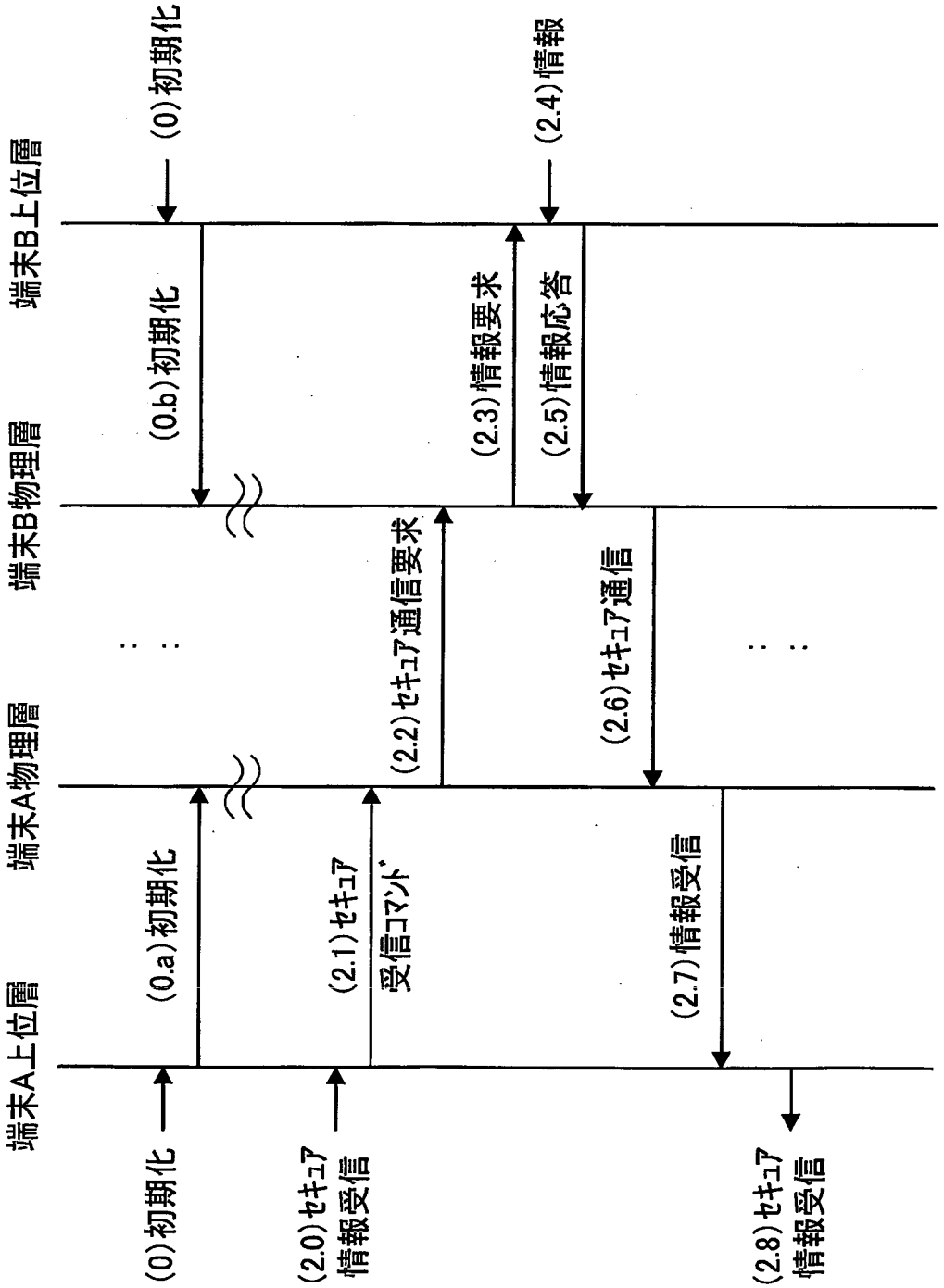

端末A上位層
端末A物理層
端末B物理層
端末B上位層
(0)初期化
(0.a)初期化
(0.b)初期化
(0)初期化
(2.0)セキュア情報受信
(2.1)セキュア受信コマンド
(2.2)セキュア通信要求
(2.3)情報要求
(2.4)情報
(2.5)情報応答
(2.6)セキュア通信
(2.7)情報受信
(2.8)セキュア情報受信

図62

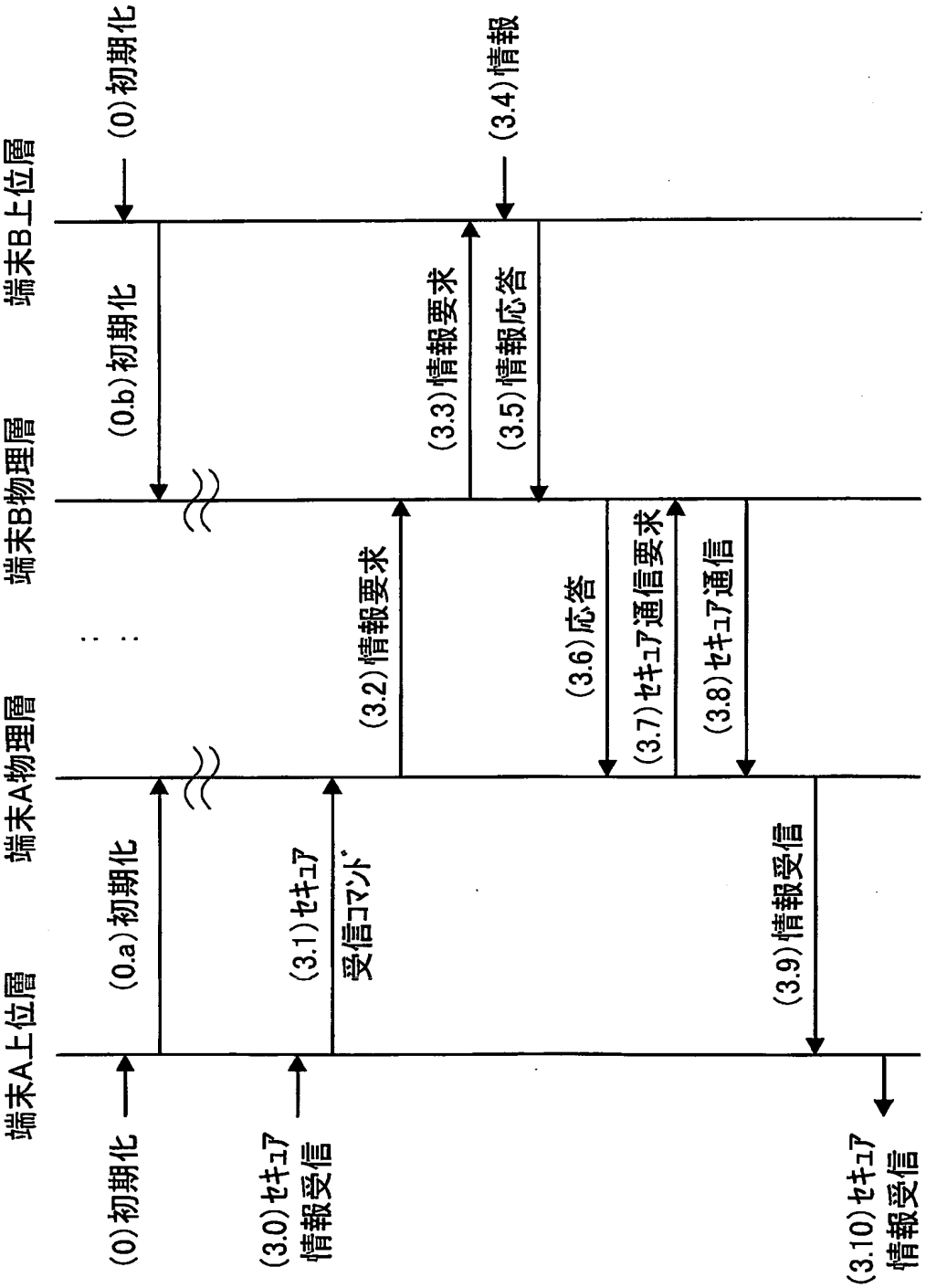

端末A上位層
端末A物理層
端末B物理層
端末B上位層
(0)初期化
(0.a)初期化
(0.b)初期化
(0)初期化
(3.0)セキュア情報受信
(3.1)セキュア受信コマンド
(3.2)情報要求
(3.3)情報要求
(3.4)情報
(3.5)情報応答
(3.6)応答
(3.7)セキュア通信要求
(3.8)セキュア通信
(3.9)情報受信
(3.10)セキュア情報受信

図63

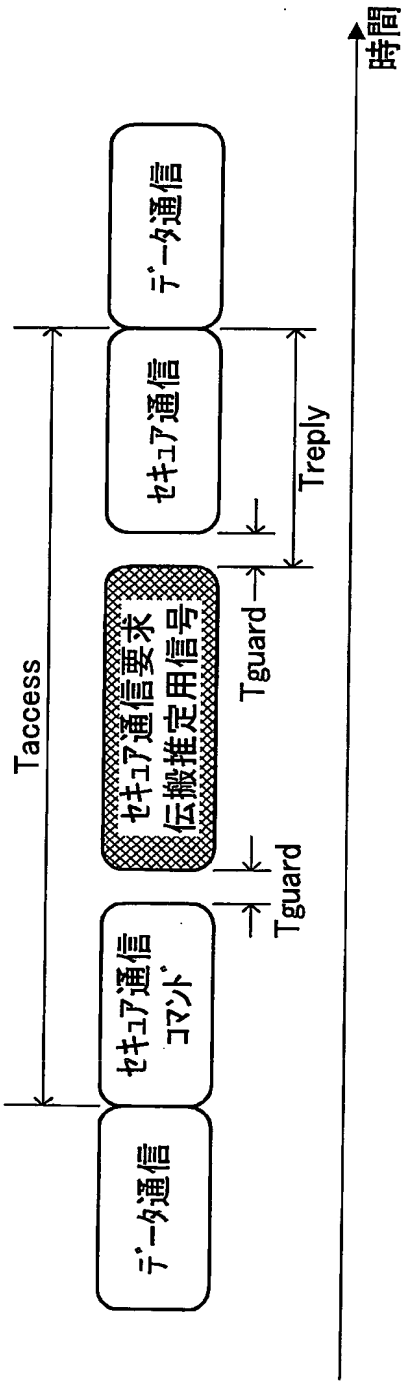

時間
データ通信
セキュア通信
セキュア通信要求
伝搬推定用信号
セキュア通信
コマンド
データ通信
Treply
Tguard
Tguard
Taccess

図64

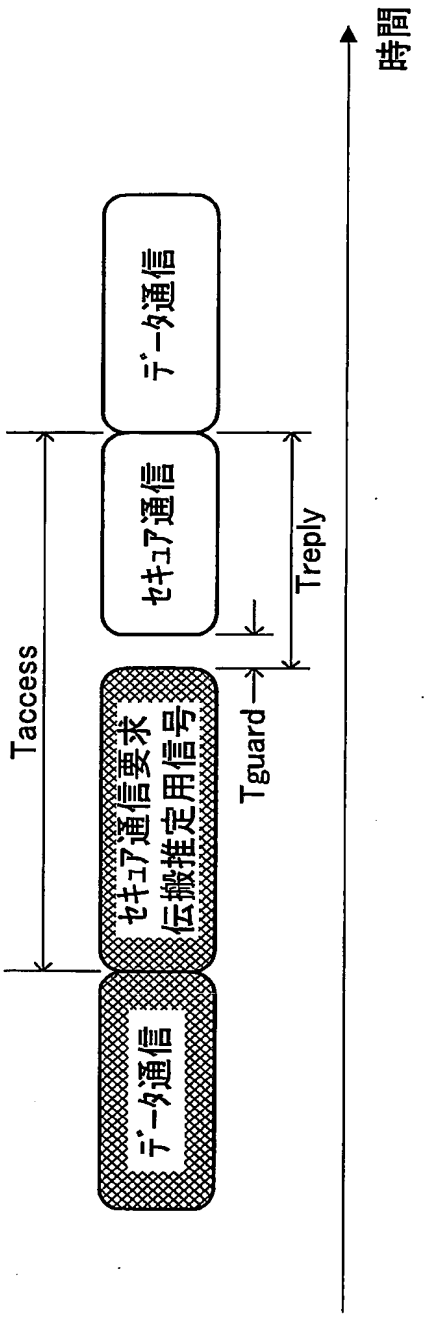

時間
データ通信
セキュア通信
セキュア通信要求
伝搬推定用信号
データ通信
Taccess
Treply
Tguard

図65

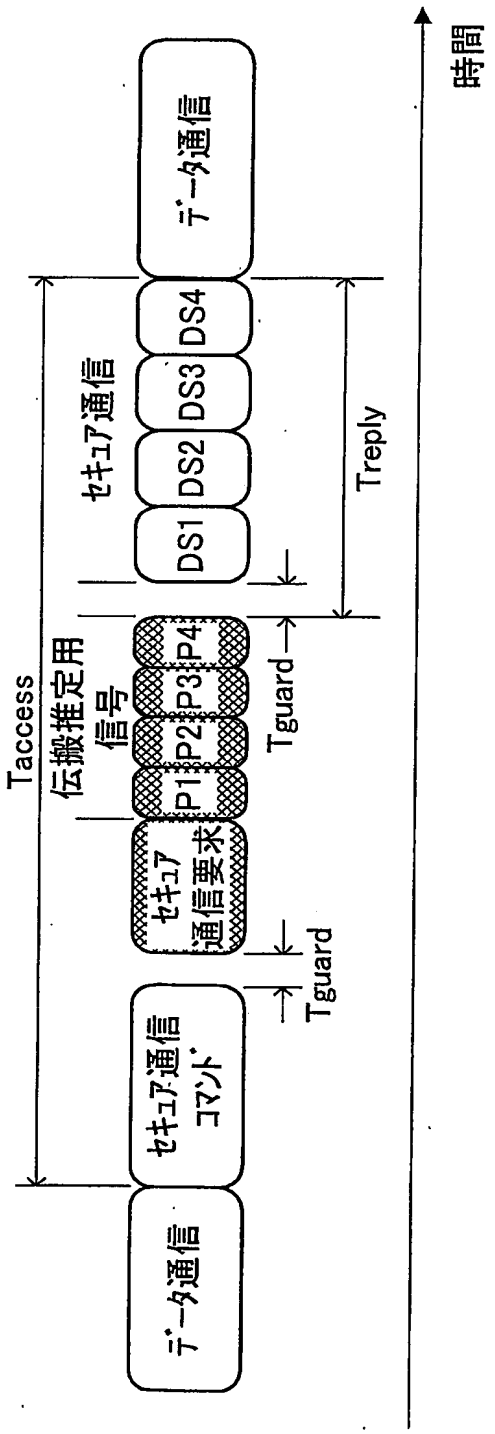

時間
Taccess
伝搬推定用信号
P1
P2
P3
P4
Tguard
セキュア通信要求
Tguard
セキュア通信コマンド
データ通信
セキュア通信
DS1
DS2
DS3
DS4
Treply
データ通信

図66

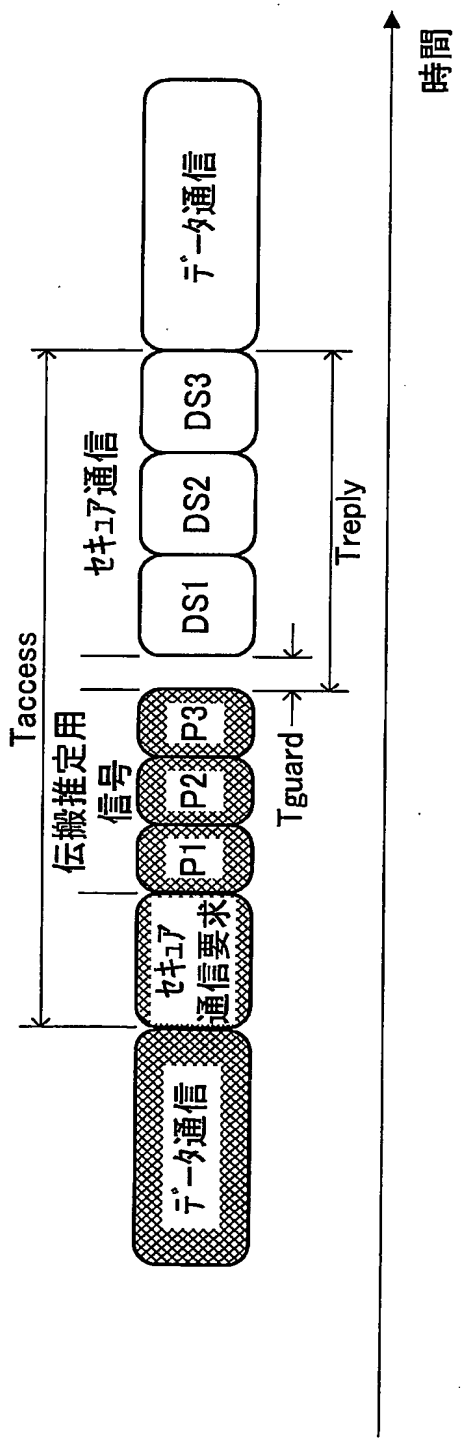

時間
データ通信
DS3
DS2
DS1
セキュア通信
Treply
Taccess
伝搬推定用信号
P3
P2
P1
Tguard
セキュア通信要求
データ通信

図67

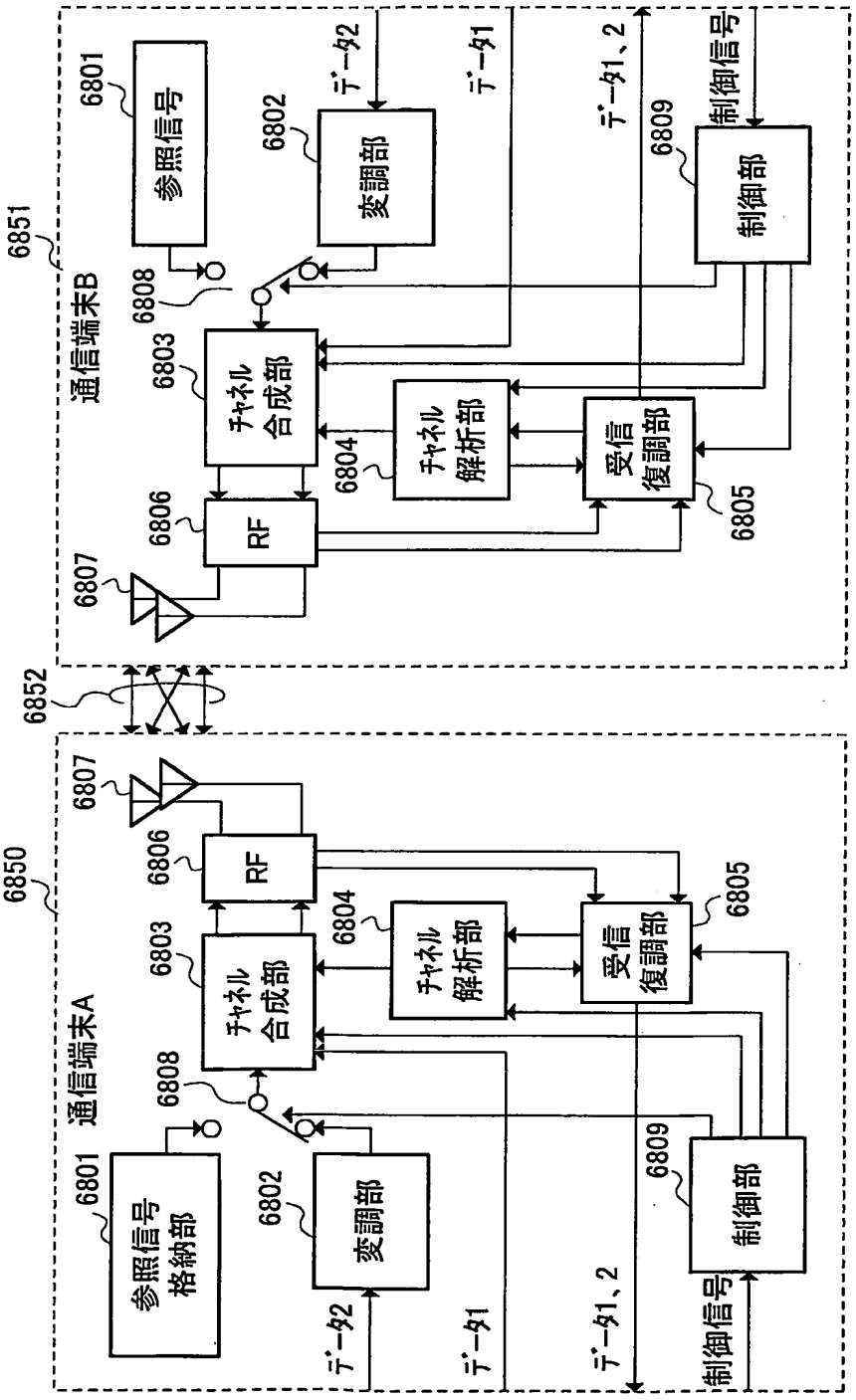

6851
通信端末B
6801
参照信号
6802
変調部
データ2
データ1
データ1、2
6809
制御信号
制御部
6808
6803
チャネル合成部
6804
チャネル解析部
受信復調部
6805
6806
RF
6807
6852
6850
通信端末A
6801
参照信号格納部
6802
変調部
データ2
データ1
データ1、2
6809
制御部
制御信号
6808
6803
チャネル合成部
6804
チャネル解析部
受信復調部
6805
6806
RF
6807

図68

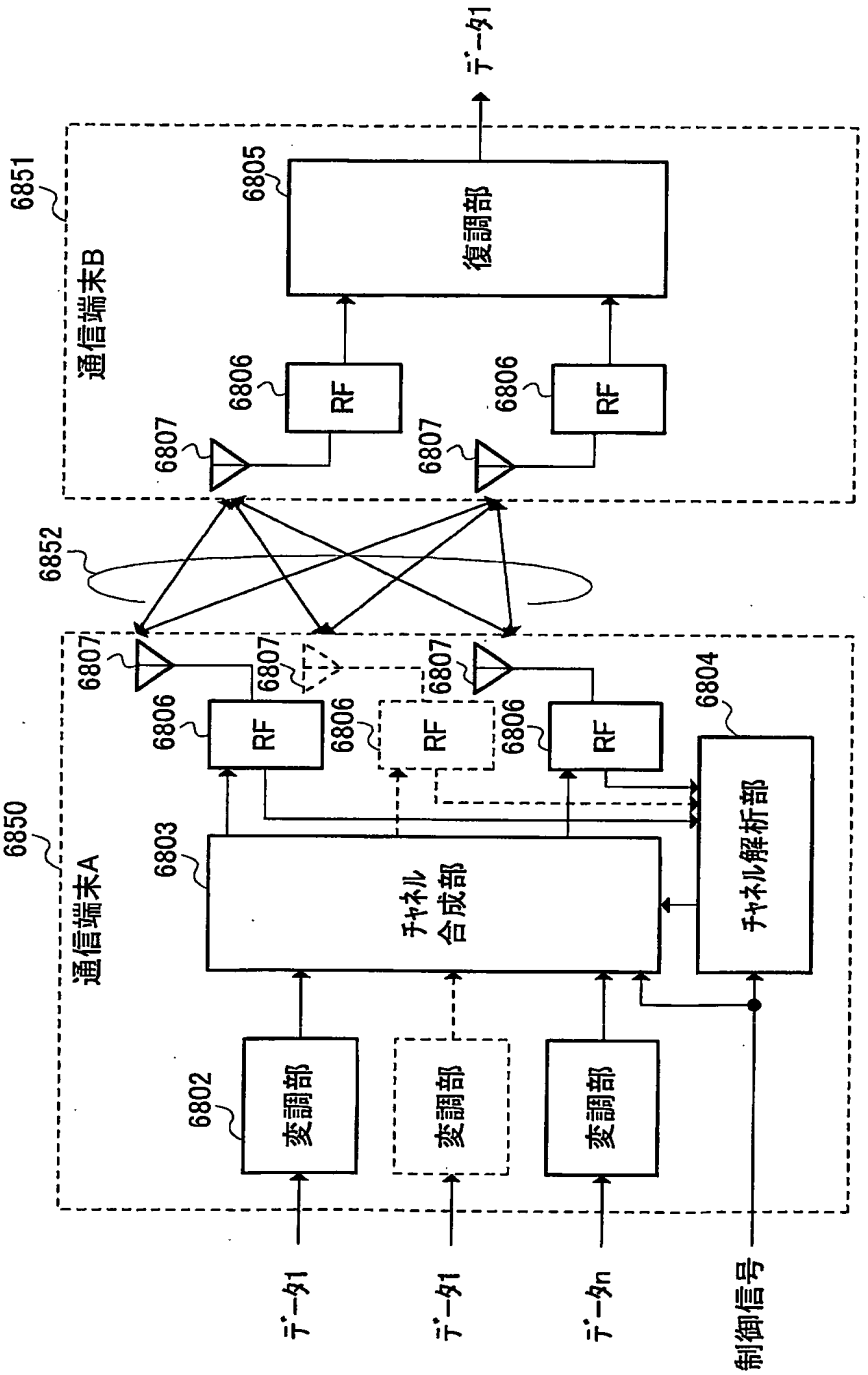

データ1
6851
通信端末B
6805
復調部
6806
RF
6806
RF
6807
6807
6852
6807
6807
6807
6806
RF
6806
RF
6806
RF
6804
6850
通信端末A
6803
チャネル合成部
チャネル解析部
6802
変調部
変調部
変調部
データ1
データ1
データn
制御信号

図69

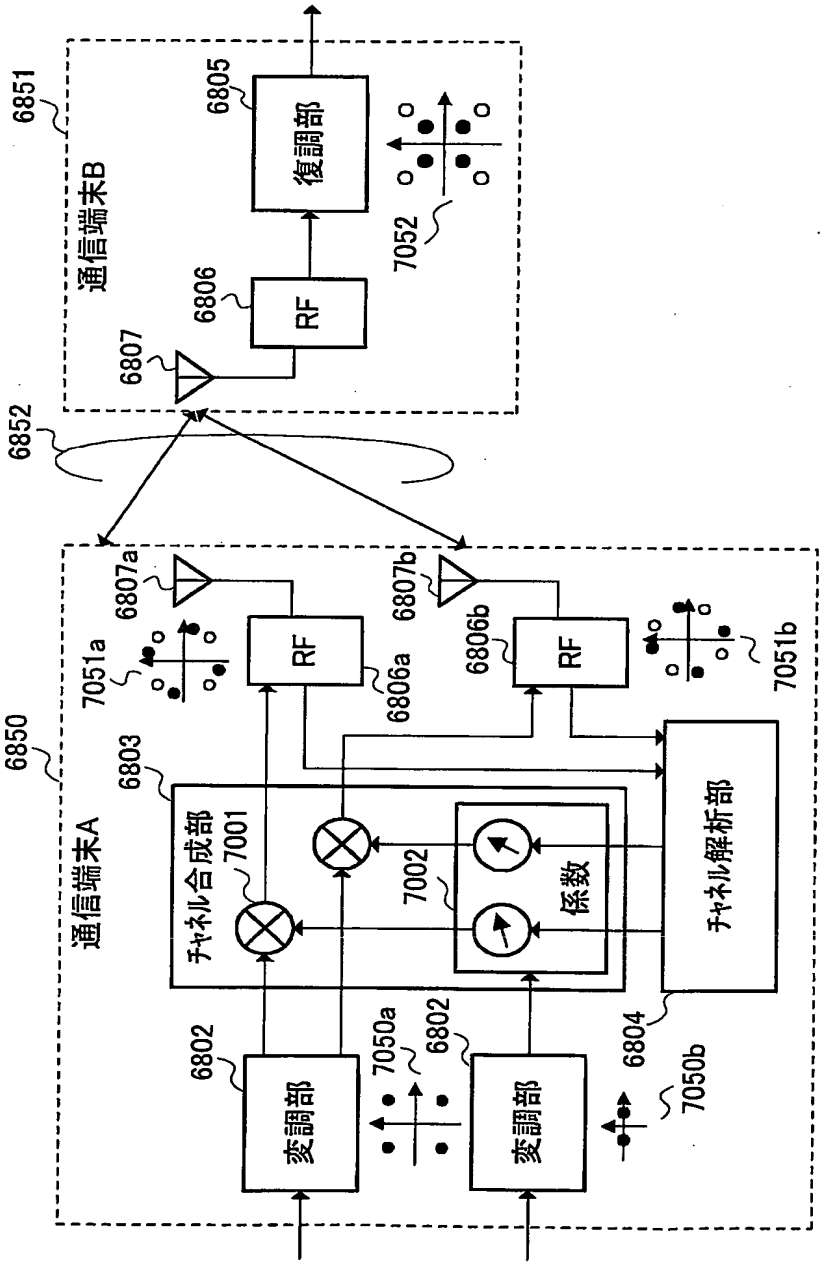

6851
通信端末B
6805
復調部
7052
6806
RF
6807
6852
6850
通信端末A
6807a
6807b
7051a
RF
6806a
6806b
RF
7051b
6803
チャネル合成部
7001
7002
係数
チャネル解析部
6802
変調部
7050a
6802
変調部
6804
7050b

図70

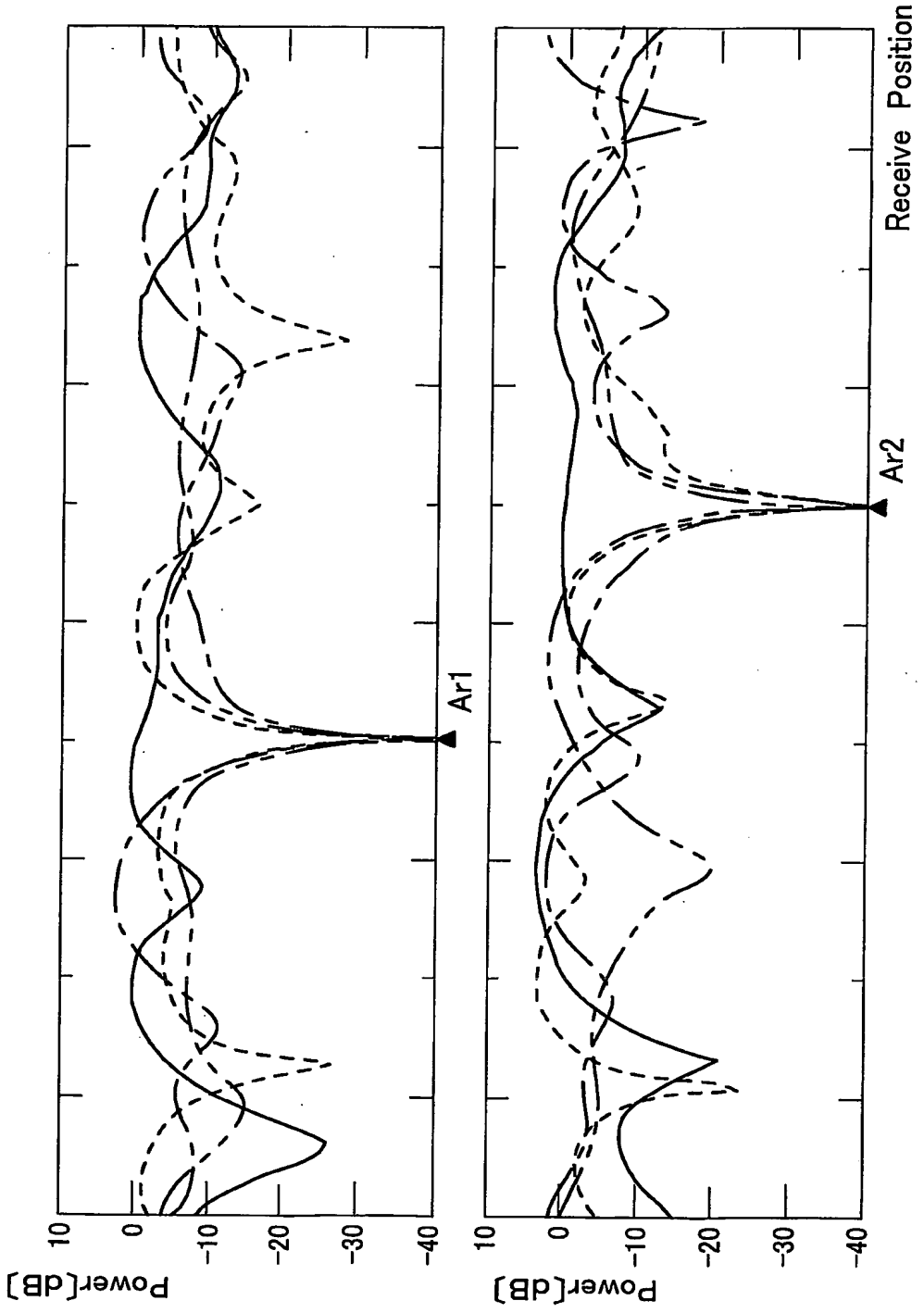

Power[dB]
10
0
-10
-20
-30
-40
Ar1
Power[dB]
10
0
-10
-20
-30
-40
Ar2
Receive Position

図71

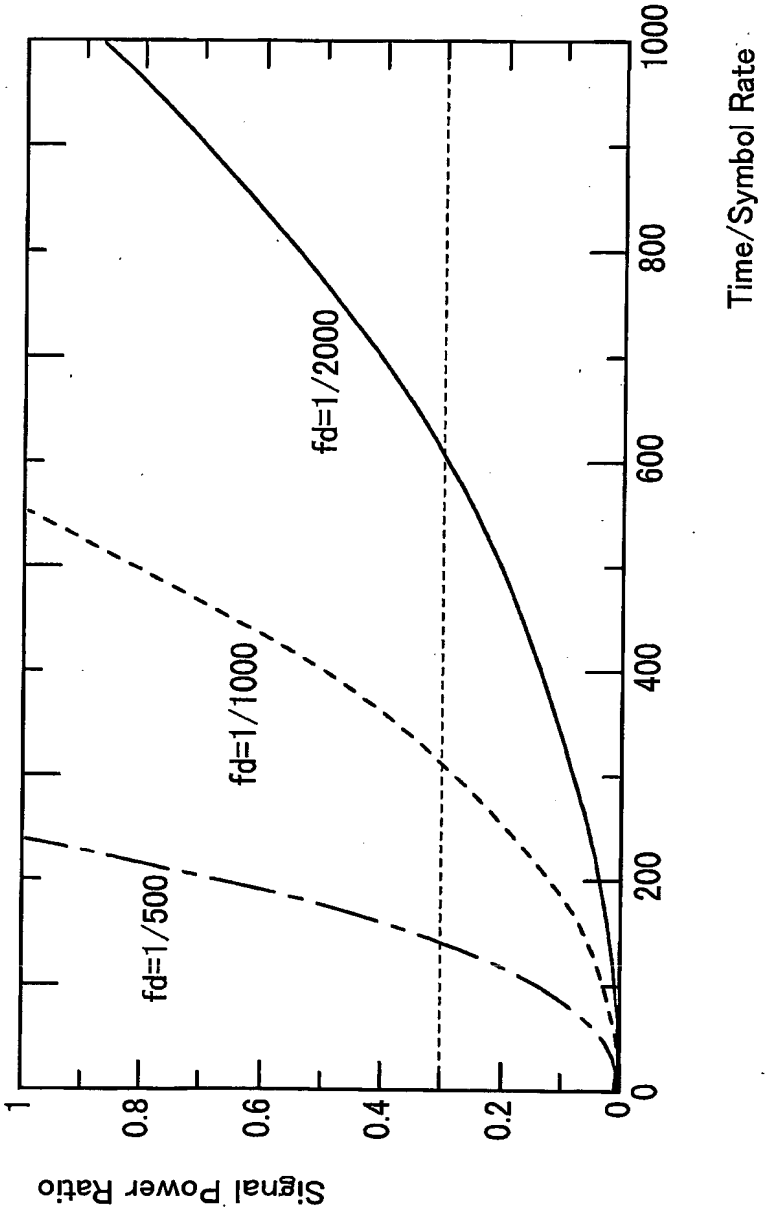

Signal Power Ratio
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
Time/Symbol Rate
fd=1/2000
fd=1/1000
fd=1/500

図72

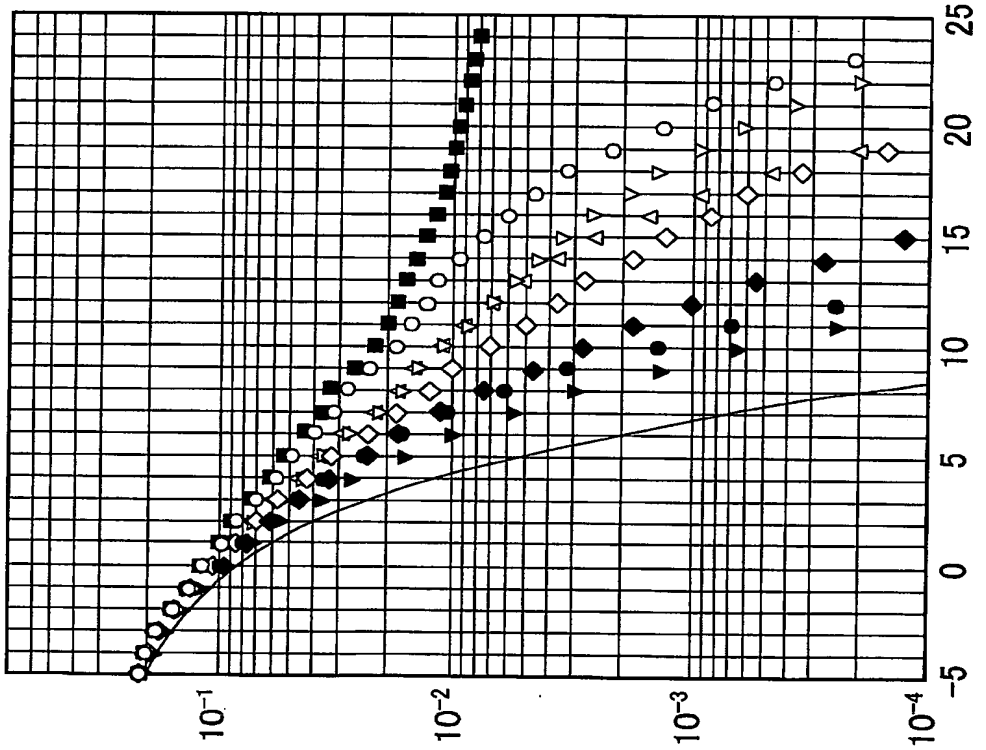


図73

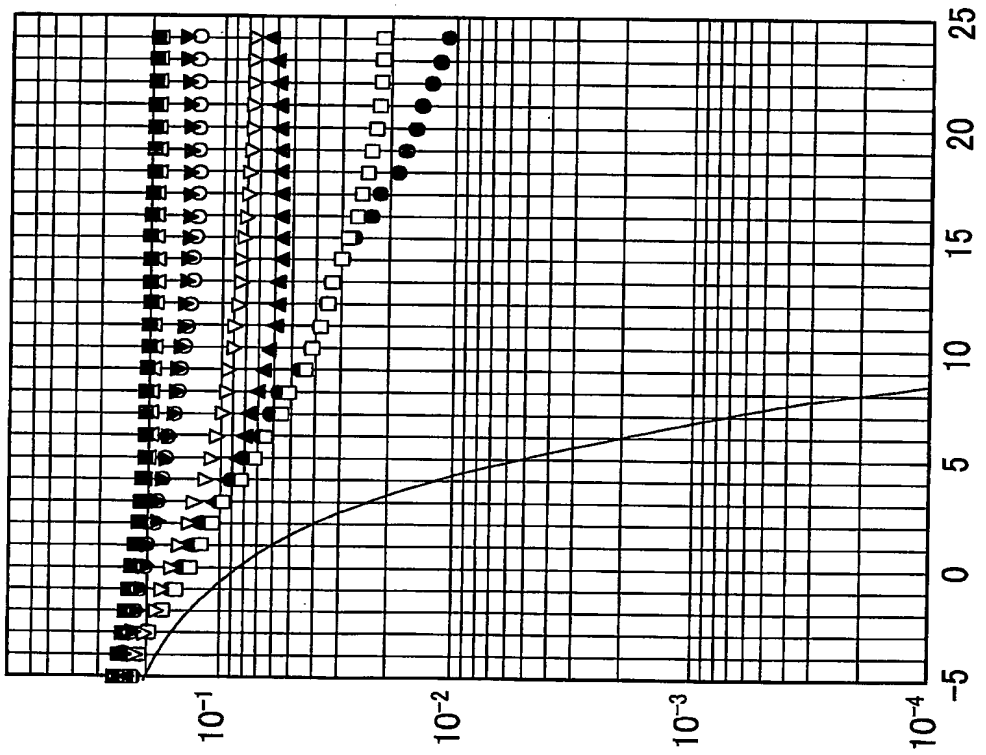


図74

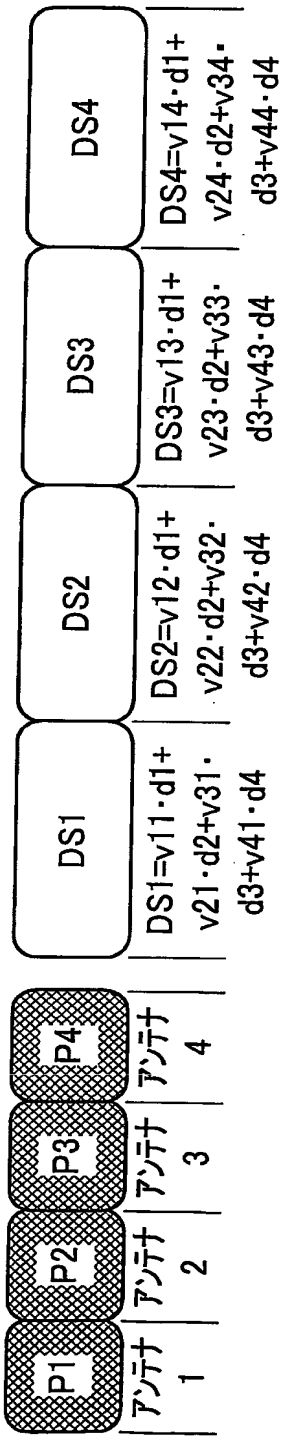

アンテナ 1
アンテナ 2
アンテナ 3
アンテナ 4
P1
P2
P3
P4
DS1
DS2
DS3
DS4
DS1=v11・d1+ v21・d2+v31・ d3+v41・d4
DS2=v12・d1+ v22・d2+v32・ d3+v42・d4
DS3=v13・d1+ v23・d2+v33・ d3+v43・d4
DS4=v14・d1+ v24・d2+v34・ d3+v44・d4

図75

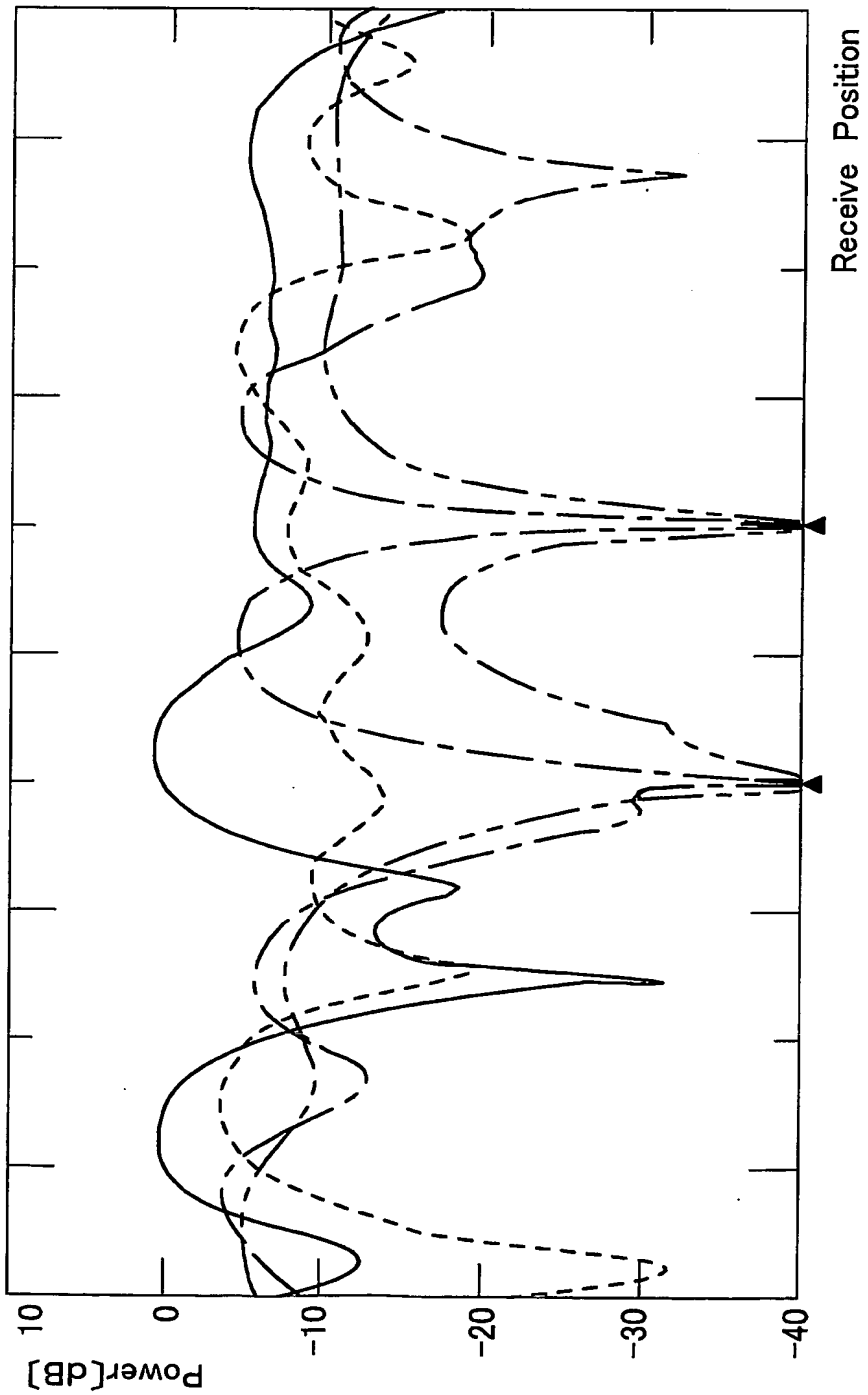


図76

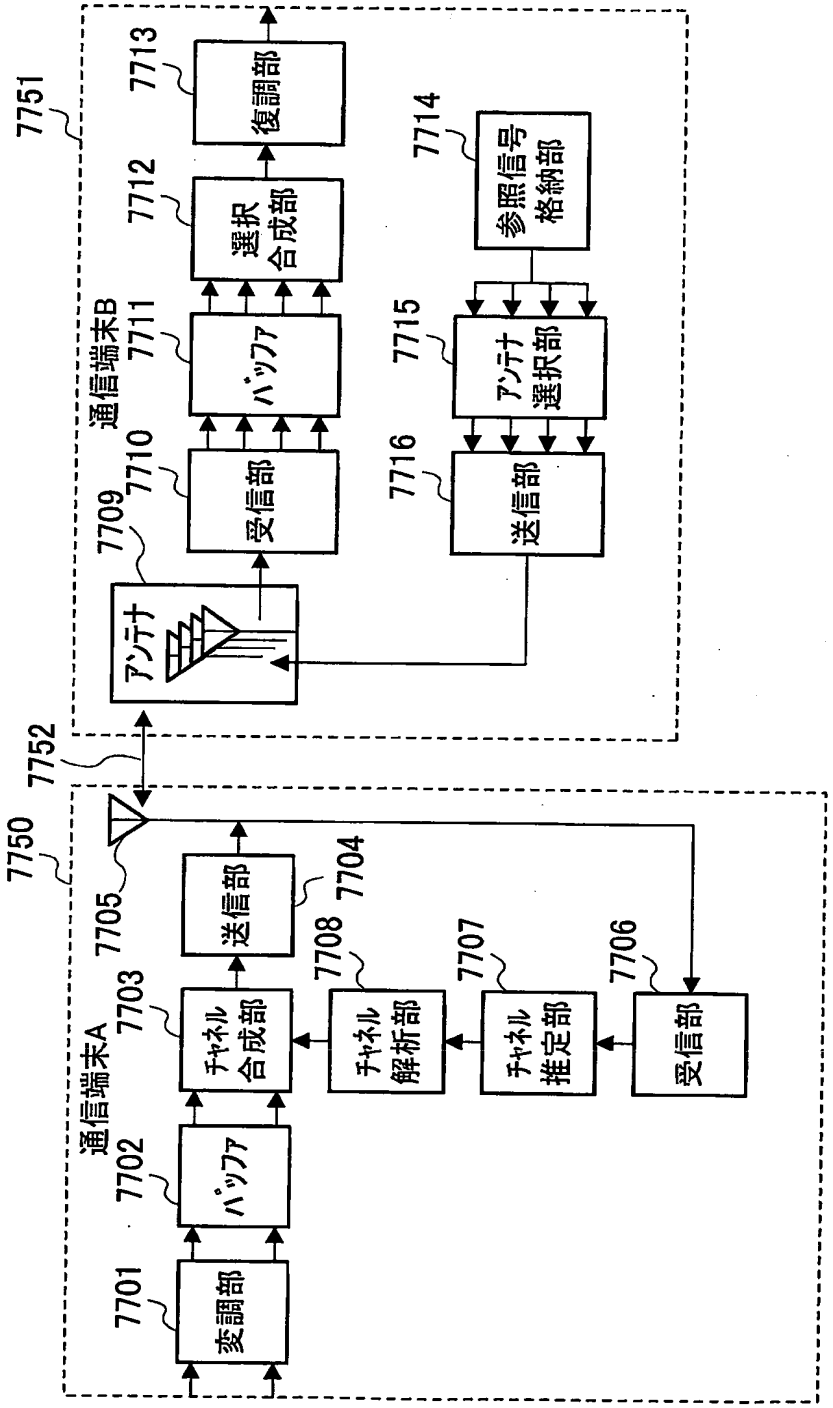

7751
7713
復調部
7712
選択
合成部
7714
参照信号
格納部
通信端末B
7711
バッファ
7715
アンテナ
選択部
7710
受信部
7716
送信部
7709
アンテナ
7752
7750
7705
送信部
7704
7708
チャネル
解析部
7707
チャネル
推定部
7706
受信部
通信端末A
7703
チャネル
合成部
7702
バッファ
7701
変調部

図77

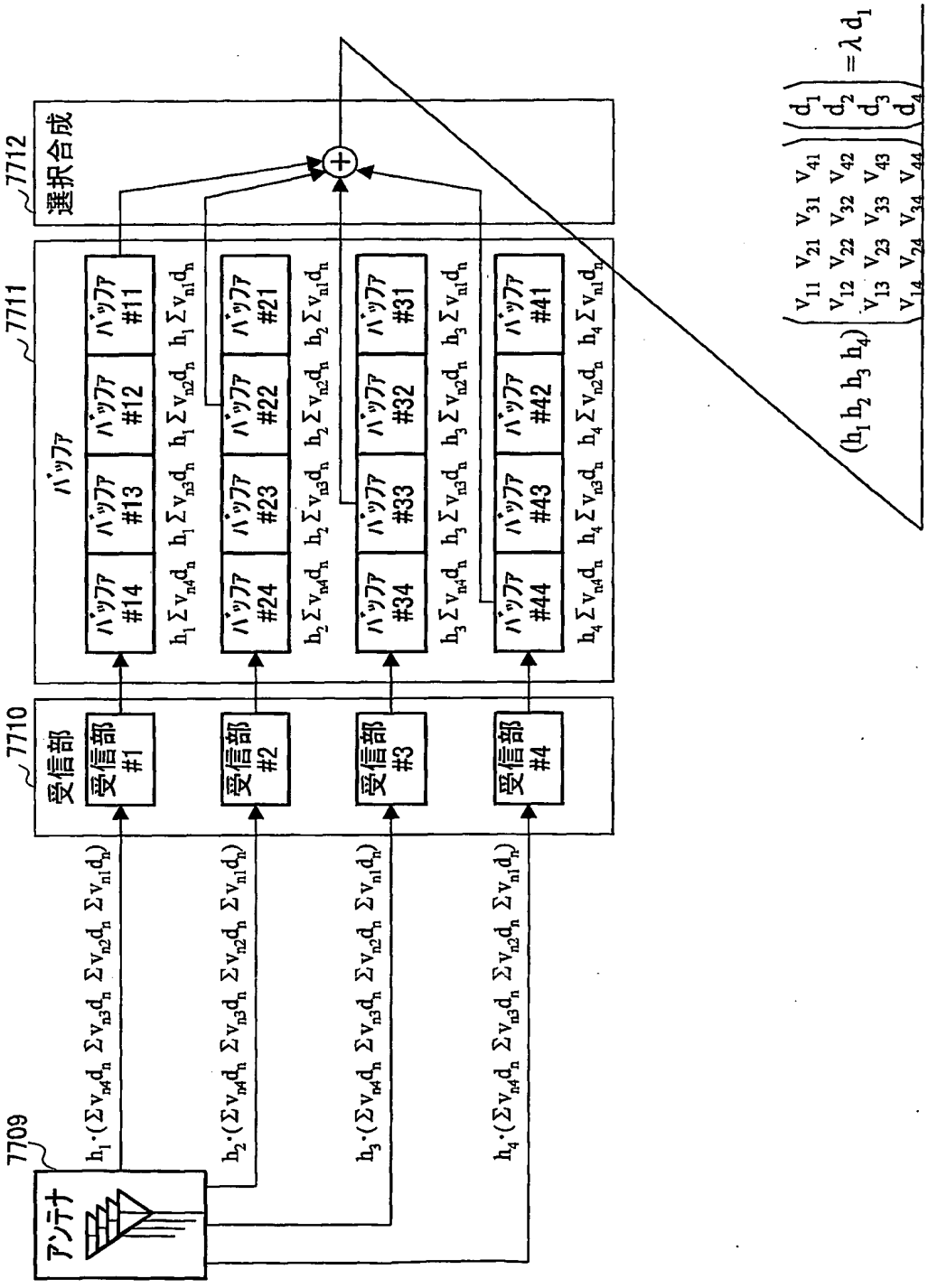

7709
アンテナ
7710
受信部
受信部 #1
受信部 #2
受信部 #3
受信部 #4
7711
バッファ
バッファ #11
バッファ #12
バッファ #13
バッファ #14
バッファ #21
バッファ #22
バッファ #23
バッファ #24
バッファ #31
バッファ #32
バッファ #33
バッファ #34
バッファ #41
バッファ #42
バッファ #43
バッファ #44
7712
選択合成
$h_1 \cdot (\Sigma v_{n4} d_n \ \Sigma v_{n3} d_n \ \Sigma v_{n2} d_n \ \Sigma v_{n1} d_n)$
$h_2 \cdot (\Sigma v_{n4} d_n \ \Sigma v_{n3} d_n \ \Sigma v_{n2} d_n \ \Sigma v_{n1} d_n)$
$h_3 \cdot (\Sigma v_{n4} d_n \ \Sigma v_{n3} d_n \ \Sigma v_{n2} d_n \ \Sigma v_{n1} d_n)$
$h_4 \cdot (\Sigma v_{n4} d_n \ \Sigma v_{n3} d_n \ \Sigma v_{n2} d_n \ \Sigma v_{n1} d_n)$
$h_1 \Sigma v_{n4} d_n \ h_1 \Sigma v_{n3} d_n \ h_1 \Sigma v_{n2} d_n \ h_1 \Sigma v_{n1} d_n$
$h_2 \Sigma v_{n4} d_n \ h_2 \Sigma v_{n3} d_n \ h_2 \Sigma v_{n2} d_n \ h_2 \Sigma v_{n1} d_n$
$h_3 \Sigma v_{n4} d_n \ h_3 \Sigma v_{n3} d_n \ h_3 \Sigma v_{n2} d_n \ h_3 \Sigma v_{n1} d_n$
$h_4 \Sigma v_{n4} d_n \ h_4 \Sigma v_{n3} d_n \ h_4 \Sigma v_{n2} d_n \ h_4 \Sigma v_{n1} d_n$
$(h_1 h_2 h_3 h_4) \begin{pmatrix} v_{11} & v_{21} & v_{31} & v_{41} \\ v_{12} & v_{22} & v_{32} & v_{42} \\ v_{13} & v_{23} & v_{33} & v_{43} \\ v_{14} & v_{24} & v_{34} & v_{44} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \lambda d_1$

図78

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/02174

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/14, H04Q7/38, H04B7/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/14, H04Q7/38, H04B7/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Chikako UCHIYAMA, "Ryoshi Rikigaku no Kiso to Ryoshi Ango Ryoshi Tsushin Channel no Shiten", Surikagaku, The December issue, Saiensu-sha Co., Ltd., No.402, 01 December, 1996 (01.12.96), pages 53 to 61	1-3,12
X	Masayoshi MUROYA, Heichi YAMAMOTO, "Digital Communication Series Digital Musen Tsushin", Sangyo Tosho Kabushiki Kaisha, 5th edition, 10 March, 1992 (10.03.92), pages 103 to 127	1,3-9,11
Y	pages 169 to 170	10
Y	JP 5-41607 A (KDD Kabushiki Kaisha), 19 February, 1993 (19.02.93), Full text; Figs. 1 to 9 & US 5218359 A	10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 22 May, 2003 (22.05.03)	Date of mailing of the international search report 03 June, 2003 (03.06.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０２１７４

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８　Ｈ０４Ｌ９／１４　Ｈ０４Ｑ７／３８　Ｈ０４Ｂ７／０６

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８　Ｈ０４Ｌ９／１４　Ｈ０４Ｑ７／３８　Ｈ０４Ｂ７／０６

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国登録実用新案公報	１９９４－２００３年
日本国実用新案登録公報	１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	内山智香子：“量子力学の基礎と量子暗号　量子通信チャンネルの視点”，数理科学　１２月号，株式会社サイエンス社，ＮＯ．４０２，１９９６．１２．０１ ｐ．５３－６１	１－３，１２
X Y	室谷正芳，山本平一：“ディジタル　コミュニケーション　シリーズ　ディジタル無線通信”，産業図書株式会社，第５版，１９９２．０３．１０ ｐ．１０３－１２７ ｐ．１６９－１７０	1, 3-9, 11 １０

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２２．０５．０３	国際調査報告の発送日　03.06.03
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木　重徳　5M　4229 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０２１７４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　５－４１６０７　Ａ（国際電信電話株式会社） １９９３．０２．１９　全文，図１－９ ＆　ＵＳ　５２１８３５９　Ａ	１０

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（１９９８年７月）